Annales du CAPES externe de Mathématiques 2006 à 2008
+ Agrégation interne 2008

= 8 problèmes corrigés

D.-J. Mercier & J.-E. Rombaldi

Table des matières

Avant-propos

S'il existe de nombreuses façons de préparer l'écrit d'un concours, l'entraînement direct sur des annales brutes est une méthode de choix qui permet de concentrer ses efforts sur des problèmes qui ont été effectivement posés les années précédentes, et ainsi de travailler sans risque de hors sujet.

Tout est au mieux si l'on se rappelle que ces problèmes sont décidément trop longs pour être résolus en cinq ou six heures, et que certaines questions sont trop difficiles pour qu'on puisse y répondre en temps limité.
Pour utiliser ces problèmes comme tremplin pour l'écrit, il s'agit donc de traiter les questions que l'on sent et éviter de rester trop longtemps sur celles qui nous résistent. Dans les deux cas, la lecture d'une solution suffisamment détaillée permettra de comparer les méthodes, de découvrir un savoir ou une pratique, ou de mettre en évidence un thème qu'il s'agira de réviser en profondeur sur des livres de cours ad hoc.

Ce recueil propose les énoncés et les solutions détaillées des six problèmes du CAPES externe de Mathématiques de la session 2006 à la session 2008. Nous avons voulu ajouter les énoncés et corrigés des deux dernières épreuves d'agrégation interne 2008 pour offrir aux candidats au CAPES la possibilité de s'entraîner sur ces problèmes récents d'un concours proche, sur des thèmes qui font aussi partie de ceux du CAPES.

Pour terminer cet avant-propos, nous voudrions recommander au lecteur de jeter un coup d'oeil sur notre site internet *MégaMaths*[1] pour :

- retrouver d'autres énoncés d'annales de concours ;

- télécharger des corrections d'annales anciennes qui permettront de continuer l'entraînement sur des "problèmes bruts" intéressants et formateurs ;

- se renseigner sur les bonus offerts pour l'achat d'une de nos annales, en particulier ceux qui proposent nos corrections de problèmes très récents du concours pour compléter sa collection en attendant l'impression du recueil d'annales suivant.

Il ne reste plus qu'à vous souhaiter du plaisir et de l'appétit devant ces huit problèmes assez longs...

D.-J. Mercier & J.-E. Rombaldi
le 6 avril 2008.

[0] [cmonannalescapesexterne2006a08] v1.05

[0] L'illustation de la couverture est de Nadine Rombaldi, et s'intitule : "Entre feu et glace".

[1] Tapez "megamaths" dans votre moteur de recherche favori !

Première partie

ANALYSE

Chapitre 1

CAPES externe 2006, épreuve 1

1.1 Énoncé

1. Présentation du jeu

1.1.Les règles du jeu

Le « tournoi » est un jeu comportant une suite de manches (appelées « duels ») opposant deux joueurs, jamais plus. Les joueurs vont entrer en jeu successivement, tant qu'aucun d'entre eux n'aura été déclaré vainqueur, et forment ainsi une suite $(J_0, J_{1,\ldots})$ aussi longue qu'il faudra, ce qui nous conduit à considérer une suite infinie de joueurs notée $(J_n)_{n\in\mathbb{N}}$.
Le premier duel oppose J_0 et J_1, le vainqueur reste en jeu et se voit opposer J_2 qui entre pour le deuxième duel. Plus généralement le n-ème duel ($n \geq 2$) oppose le joueur J_n, qui entre alors en jeu, au vainqueur du duel précédent, le perdant quittant le jeu.
On convient enfin que le premier joueur qui remporte N duels, nécessairement consécutifs, est déclaré vainqueur et que le jeu prend fin. N est un entier fixé à l'avance, au moins égal à 2, et valable pour tout le déroulement du tournoi.
Le but de ce problème est de rendre compte de ce type de jeu en proposant diverses modélisations probabilistes. On s'intéressera plus particulièrement à la durée du jeu, c'est-à-dire au nombre de duels ayant lieu avant la proclamation du vainqueur.

1.2. Les règles communes aux différentes modélisations aléatoires

La succession des duels est parfaitement décrite si on connaît, pour chacun, les numéros des participants et le numéro du gagnant, cela tant que le jeu

continue, c'est-à-dire tant qu'aucun des joueurs n'a été déclaré vainqueur. On supposera que chaque duel est un jeu de hasard, on considérera ainsi le n-ème duel comme une épreuve aléatoire $\mathcal{E}_n$, dont on observera les résultats possibles. On présupposera, sans chercher à l'expliciter, l'existence d'un espace probabilisé $(\Omega, \mathcal{A}, \mathbb{P})$ permettant de modéliser le jeu et on s'attachera à décrire l'univers des possibles, c'est-à-dire les issues des différentes épreuves, ainsi que la manière dont on affecte des probabilités aux résultats observés. Les modèles proposés devront respecter les règles suivantes :

1. Le premier duel : la probabilité que le résultat de $\mathcal{E}_1$ soit 1 (J_1 est le gagnant du premier duel) est p, où p est un élément de $]0,1[$ fixé dans tout le problème, le résultat étant 0 avec la probabilité $1-p$.
2. Les duels successifs :
   (a) Pour $n \geq 2$, l'épreuve $\mathcal{E}_n$, si elle a lieu, ne dépend que de celles qui l'ont précédées que par le numéro du joueur opposé à J_n (celui qui a remporté le duel précédent).
   (b) La probabilité pour J_n de remporter ce duel (le résultat est n) est égale à p_n, où $(p_k)_{k\geq 2}$ est une suite d'éléments de $]0,1[$, le joueur qui lui est opposé étant vainqueur avec une probabilité $1-p_n$.

On admettra, par ailleurs que, pour toute suite $(\mathcal{A}_n)_{n\in\mathbb{N}}$ d'événements disjoints et dont la réunion est de probabilité 1, il existe une variable aléatoire X à valeurs dans $\mathbb{N}$ vérifiant :

$$\forall n \in \mathbb{N},\ \mathbb{P}\left(X = n\right) = \mathbb{P}\left(\mathcal{A}_n\right).$$

2. Préliminaires

On se propose ici de démontrer divers résultats qui pourront être utilisés dans la suite du problème.

2.1 Résultat 1

$(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont deux suites à termes positifs vérifiant :

$$x_n \underset{n\to+\infty}{\backsim} y_n$$

1. Justifier, pour tout ε strictement positif, l'existence d'un entier naturel non nul n_0 tel que pour tout n supérieur ou égal à n_0, on ait :

$$\left|\sum_{k=0}^{n} x_k - \sum_{k=0}^{n} y_k\right| \leq \left|\sum_{k=0}^{n_0-1} (x_k - y_k)\right| + \varepsilon \sum_{k=n_0}^{n} x_k$$

2. En déduire que, si la série de terme général x_n est divergente, on a :

$$\sum_{k=0}^{n} x_k \underset{n\to+\infty}{\backsim} \sum_{k=0}^{n} y_k$$

2.2 Résultat 2

1. $(u_n)_{n\in\mathbb{N}}$ est une suite à termes positifs telle que la série de terme général u_n soit convergente.

   (a) Montrer qu'on définit une suite de réels par la relation :

   $$\forall n \in \mathbb{N},\ v_n = \sum_{k=n+1}^{+\infty} u_k$$

   Quelle est la nature de cette suite ?

   (b) Justifier pour tout entier naturel n non nul :

   $$\sum_{k=1}^{n} k u_k = \sum_{k=0}^{n-1} v_k - n v_n.$$

   (c) Montrer que si la série de terme général v_n est convergente, alors la série de terme général nu_n est convergente.

   (d) Montrer que si la série de terme général nu_n est convergente, alors la suite de terme général nv_n est convergente.

   (e) En déduire que les séries de termes généraux respectifs nu_n et v_n sont ou bien convergentes de même somme, ou bien toutes les deux divergente.

2. Dans cette question, X désigne une variable aléatoire définie sur un espace de probabilité $(\Omega, \mathcal{A}, \mathbb{P})$ prenant ses valeurs dans $\mathbb{N}$. Déduire de ce qui précède qu'elle admet une espérance si, et seulement si, la série de terme général $\mathbb{P}(X > n)$ est convergente et qu'on a alors l'égalité :

$$\mathbb{E}(X) = \sum_{n=0}^{+\infty} \mathbb{P}(X > n).$$

2.3 Résultat 3

$(a_n)_{n\in\mathbb{N}}$ est une suite à termes positifs telle que la série entière $\sum a_n x^n$ admette un rayon de convergence R strictement positif. On note :

$$\forall x \in \left]-R, R\right[,\ f(x) = \sum_{n\geq 0} a_n x^n$$

1. Montrer que la fonction $f(x)$ admet une limite finie lorsque x tend vers R sur $[0, R[$ si, et seulement si, f est majorée sur $[0, R[$.
   On suppose dans la suite de cette partie que l'une de ces conditions équivalentes est réalisée et on note L la limite.
2.
   (a) Montrer que, pour tout n entier naturel :
   $$\sum_{k=0}^{n} a_k R^k \leq L.$$
   (b) En déduire que la série de terme général $a_n R^n$ est convergente.
   (c) Montrer que la série entière $\sum a_n x^n$ est normalement convergente sur $[-R, R]$. En déduire que :
   $$\sum_{n=0}^{+\infty} a_n R^n = \lim_{x \to R^-} f(x).$$

3. Première modélisation : le cas particulier $N = 2$

Dans cette section on observe la suite des différents vainqueurs successifs. L'univers des possibles est alors l'ensemble des listes (éventuellement infinies) représentant les numéros des joueurs vainqueurs aux différents duels. Ainsi : $(0, 2, 3, 3)$ représentera un jeu de 4 duels remportés successivement par J_0, J_2, J_3 et J_3 qui est alors déclaré gagnant du tournoi, ce qui met fin à celui-ci. On note D_n, pour n au moins égal à 2, l'événement « le jeu s'arrête à l'issue du n-ème duel ».

1.
   (a) Expliciter D_2 à l'aide de la modélisation proposée.
   (b) Plus généralement, expliciter D_{n+1} lorsque n est un entier au moins égal à 2.
2. Dans cette question on suppose que, pour tout $n \geq 2$, p_n est égal à p.
   (a) Calculer $\mathbb{P}(D_n)$ pour n supérieur ou égal à 2. Vérifier que $\bigcup_{n=2}^{+\infty} D_n$ est un événement de probabilité 1. Interpréter ce résultat.
   (b) On peut alors considérer une variable aléatoire T égale au nombre de duels qui ont effectivement eut lieu lorsque le jeu s'arrête. Calculer, après avoir justifié leurs existences, son éspérance et sa variance.

3. On revient au cas général où pour i au moins égal à 2, p_i est un réel élément de $]0,1[$. On pose pour tout n au moins égal à 2 :

$$\beta_n = \prod_{i=2}^{n} p_i$$

Exprimer, pour n au moins égal à 2, $\sum_{k=2}^{n} \mathbb{P}(D_k)$ en fonction de la suite $(\beta_k)_{k\geq 2}$. En déduire que $\bigcup_{k=2}^{n} D_k$ est un événement de probabilité 1 si, et seulement si, β_n tend vers 0 lorsque n tend vers l'infini.
Lorsque cette condition est vérifiée on définira T comme à la question **2.b.** et on posera, pour $n \geq 2$:

$$u_n = \beta_n - \beta_{n+1}$$

Jusqu'à la fin de cette section **3.** on suppose qu'il existe un réel α strictement positif tel que pour tout i au moins égal à 2, l'égalité suivante soit vérifiée :

$$p_i = 1 - \frac{1}{i^\alpha}$$

4. Donner une condition nécessaire et suffisante sur α pour que $\bigcup_{n=2}^{+\infty} D_n$ soit un événement de probabilité 1.
Indication : on pourra s'intéresser à la suite de terme général $-\ln(\beta_n)$.
5. Dans cette question, α est égal à 1. Donner une loi de T. T admet-elle une espérance ?
6. Dans cette question on suppose : $0 < \alpha < 1$.
   (a) Justifier l'équivalence lorsque n tend vers l'infini :

$$\sum_{k=2}^{n} (-\ln(p_k)) \underset{+\infty}{\sim} \sum_{k=2}^{n} \frac{1}{k^\alpha}.$$

   (b) Après avoir justifié pour tout entier k au moins égal à 2 l'inégalité :

$$\frac{1}{k^\alpha} \leq \int_{k-1}^{k} \frac{dx}{x^\alpha} \leq \frac{1}{(k-1)^\alpha}$$

   démontrer l'équivalence lorsque n tend vers l'infini :

$$\sum_{k=2}^{n} \frac{1}{k^\alpha} \underset{+\infty}{\sim} \frac{n^{1-\alpha}}{1-\alpha}.$$

(c) En déduire que, pour tout réel c strictement positif, la suite de terme général $\ln(n^c u_n)$ tend vers $-\infty$ puis que la série de terme général nu_n est convergente.
Que peut-on en conclure pour l'espérance de T ?

4. Deuxième modélisation : le cas où les probabilités sont constantes

Dans cette section et jusqu'à la fin du problème N est un entier supérieur ou égal à 3 et on suppose, pour tout n supérieur ou égal à 2 : $p_n = p$. On notera $q = 1 - p$.
Pour tout n entier naturel, on note A_n l'événement « le joueur J_n participe à au moins un duel » et G_n l'événement « le joueur J_n est vainqueur du tournoi ».

4.1. Cas particulier : $N = 3$ et $p = \frac{1}{2}$

1. Montrer que :

$$\forall n \in \mathbb{N},\ \mathbb{P}(G_n) = \frac{1}{8}\mathbb{P}(A_n)$$

2. Montrer que les événements A_0, A_1, A_2 et A_3 sont des événements certains.

3.

(a) Dans cette question, n est un entier supérieur ou égal à 4. On introduit les événements $A_{n,k}$ « le n-ème duel a lieu et oppose J_n à J_{n-k} ». Montrer que la probabilité de $A_{n,k}$ est nulle si k est différent de 1 ou de 2.
En déduire alors pour $n \geq 4$:

$$\mathbb{P}(A_n) = \frac{1}{2}\mathbb{P}(A_{n-1}) + \frac{1}{4}\mathbb{P}(A_{n-2}).$$

(b) On désigne par r_1 et r_2 ($r_1 < r_2$) les deux racines de l'équation :

$$r^2 - \frac{1}{2}r - \frac{1}{4}$$

Vérifier que, pour $n \geq 2$, on a :

$$\mathbb{P}(A_n)\frac{4}{\sqrt{5}}\left(r_2^n - r_1^n\right)$$

(c) En déduire que la probabilité que le jeu s'arrête est égale à 1. On pourra alors considérer une variable aléatoire T égale au nombre de duels qui ont effectivement eut lieu lorsque le jeu s'arrête.
Calculer $\mathbb{P}(T = 3)$.
Montrer que, pour $n \geq 4$:

$$\mathbb{P}(T = n) = \mathbb{P}(G_{n-2})$$

En déduire une expression de $\mathbb{P}(T = n)$ pour $n \geq 4$ puis l'espérance de T.
Indication : Pour **4.1.3.b.** et **4.1.3.c.** il pourra être intéressant de mener formellement dans un premier temps les calculs en fonction de r_1 et de r_2 et d'utiliser ensuite leur somme et leur produit.

4.2. Étude du cas général
On revient au cas général : $N \geq 3$ et p est élément de $]0,1[$. On posera de plus, pour n entier naturel :

$$a_n = \mathbb{P}(A_n) \text{ et } g_n = \mathbb{P}(G_n)$$

1.

(a) Calculer g_0. Que vaut a_k pour $0 \leq k \leq N$.

(b) Montrer que la série de terme général g_n est convergente.

(c) Justifier, pour tout n non nul, la relation :

$$g_n = p(1-p)^{N-1} a_n$$

En déduire que la série de terme général a_n est convergente. On posera :

$$S = \sum_{n=1}^{+\infty} a_n$$

2.

(a) En considérant à nouveau les événement $A_{n,k}$ définis dans la partie précédente, justifier, pour n strictement supérieur à N, la relation :

$$a_n = \sum_{k=1}^{N-1} p(1-p)^{k-1} a_{n-k}$$

Exprimer a_{N+1} en fonction de p et de N.

(b) En sommant les égalités précédentes, montrer l'égalité :

$$(1-p)^{N-1} S = \sum_{n=1}^{N} a_n - \sum_{k=1}^{N-1} \sum_{i=k}^{N-1} p\,(1-p)^{k-1} a_{N-i}$$

En utilisant une interversion d'indices dans la somme double, puis la question **1.a.** calculer S.
En déduire la somme de la série de terme général g_n, puis que la probabilité que le jeu se termine est égale à 1.

3. On notera T une variable aléatoire égale au nombre de duels ayant eut lieu jusqu'à l'arrêt du jeu.

   (a) Exprimer a_n et g_n en fonction de T.

   (b) En utilisant le résultat **2.** des préliminaires montrer que T admet une espérance et donner l'expression de $\mathbb{E}(T)$ en fonction de p et de N. Retrouver le résultat relatif à $\mathbb{E}(T)$ de la question **4.1.3.c.** La formule obtenue vaut aussi pour $N = 2$; retrouver ainsi le résultat de la question **3.2.b.**

   (c) Démontrer, pour $n \geq N+1$:

$$a_n - a_{n+1} = p\,(1-p)^{N-1} a_{n-N+1}. \qquad (\mathcal{R})$$

5. Comportement asymptotique de la loi de T

5.1. Un lemme

Démontrer que, pour tout entier naturel r non nul et toute famille $(z_1, \cdots, z_r)$ de complexes non nuls, l'égalité :

$$\left| \sum_{k=1}^{r} z_k \right| = \sum_{k=1}^{r} |z_k|$$

n'est réalisée que lorsque :

$$\forall k \in \mathbb{N},\ (2 \leq k \leq r) \Rightarrow (\exists \lambda_k \in]0, +\infty[\,,\ z_k = \lambda_k z_1)$$

5.2. Étude d'une fonction associée à T

1. Montrer qu'on peut définir une fonction Q par :

$$\forall x \in]-1, 1[\,,\ Q(x) = \sum_{n=0}^{+\infty} \mathbb{P}(T > n)\, x^n$$

   Vérifier qu'elle est continue sur $[-1, 1]$ et dérivable sur $]-1, 1[$.

2. En utilisant la relation $(\mathcal{R})$ et en s'inspirant des techniques de calcul mises en œuvre à la question **2.b.** de la section **4.2.** démontrer, pour tout x de $[-1, 1]$, la formule :

$$\left(1 - x + \frac{p}{1-p}\left(x\left(1-p\right)\right)^N\right) Q\left(x\right) = 1 - \left(x\left(1-p\right)\right)^N.$$

3. Vérifier que les deux polynômes

$$1 - X + \frac{p}{1-p}\left(X\left(1-p\right)\right)^N \text{ et } 1 - \left(X\left(1-p\right)\right)^N$$

admettent dans $\mathbb{C}$ une seule racine commune et que celle-ci est simple et réelle. En déduire la relation :

$$Q\left(x\right) = 1 - \frac{1}{p} - \frac{1}{pB\left(x\right)} \text{ avec } B\left(x\right) = \sum_{k=1}^{N-1} p\left(1-p\right)^{k-1} x^k - 1$$

5.3. Étude des racines de B

1. Étudier les variations de B sur $\mathbb{R}^+$. Calculer $B(1)$. En déduire que B admet une unique racine réelle positive ρ_N élément de $]1, +\infty[$ et que cette racine est simple.
2. En utilisant le lemme, montrer que les racines complexes de B sont de module strictement supérieur à ρ_N.
3. D'après ce qui précède, les pôles de Q sont en particulier de module strictement supérieur à 1. Aurait-on pu prévoir directement ce résultat ?

5.4. Recherche d'équivalents

On note $\{z_1, \cdots, z_m\}$ les racines de B dans $\mathbb{C}$ de multiplicités respectives ν_k.

1. Justifier l'existence d'une famille de complexes non nuls telle que, pour tout complexe z de module inférieur ou égal à 1 on ait :

$$\frac{1}{B\left(z\right)} = \sum_{k=1}^{m} \sum_{s=1}^{\nu_k} \frac{\lambda_{k,s}}{\left(z - z_k\right)^s}$$

2. Dans cette question s et k sont fixés et z désigne un complexe de module inférieur ou égal à 1.

   (a) Justifier l'égalité :

$$\frac{1}{\left(z_k - z\right)^s} = \sum_{n=0}^{+\infty} C_{n+s-1}^{s-1} \frac{z^n}{z_k^{n+s}}$$

(b) En déduire, pour tout k, l'existence d'un polynôme P_k de degré inférieur ou égal à $\nu_k - 1$ tel que :

$$\sum_{s=1}^{\nu_k} \frac{\lambda_{k,s}}{(z - z_k)^s} = \sum_{n=0}^{+\infty} \left(\frac{P_k(n)}{z_k^n} \right) z^n$$

(c) En déduire une expression de a_{n+1} pour $n \geq 1$.

3.

(a) Montrer, à l'aide des questions précédentes, l'existence d'un réel K tel qu'on ait :

$$a_{n+1} \underset{+\infty}{\backsim} \frac{K}{\rho_N^n}$$

(b) Donner une expression de K en fonction de p, B et ρ_N. En déduire un équivalent à l'infini de $\mathbb{P}(T = n)$.

1.2 Corrigé

2. Préliminaires

2.1 Résultat 1

On rappelle que les suites réelles $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont équivalentes si, et seulement si, il existe un entier naturel n_1 et une suite réelle $(\varepsilon_n)_{n\geq n_1}$ convergente vers 0 tels que :

$$\forall n \geq n_1,\ y_n = (1 + \varepsilon_n) x_n$$

ce qui revient à dire que, pour tout réel $\varepsilon > 0$ il existe un entier naturel n_0 tel que :

$$\forall n \geq n_0,\ |y_n - x_n| \leq \varepsilon |x_n|.$$

1. Si les suites à termes positifs $(x_n)_{n\in\mathbb{N}}$ et $(y_n)_{n\in\mathbb{N}}$ sont équivalentes, pour tout réel $\varepsilon > 0$ on peut trouver un entier $n_0 \geq 1$ tel que :

$$\forall k \geq n_0,\ |x_k - y_k| \leq \varepsilon x_k.$$

On en déduit alors que pour tout $n \geq n_0$, on a :

$$\begin{aligned}
\left| \sum_{k=0}^{n} x_k - \sum_{k=0}^{n} y_k \right| &\leq \left| \sum_{k=0}^{n_0-1} (x_k - y_k) \right| + \sum_{k=n_0}^{n} |x_k - y_k| \\
&\leq \left| \sum_{k=0}^{n_0-1} (x_k - y_k) \right| + \varepsilon \sum_{k=n_0}^{n} x_k
\end{aligned}$$

2. On note $S_n = \sum\limits_{k=0}^{n} x_k$ et $T_n = \sum\limits_{k=0}^{n} y_k$ les sommes partielles d'ordre n des séries $\sum x_n$ et $\sum y_n$. Si la série à termes positifs $\sum x_n$ diverge, on a alors $\lim\limits_{n\to+\infty} S_n = +\infty$ et pour $\varepsilon > 0$ donné comme dans la question précédente, on peut choisir un entier $n_0 \geq 1$ tel que l'on ait de plus $S_n > 0$ pour tout $n \geq n_0$. L'inégalité précédente, pour $n \geq n_0$, s'écrit alors :

$$\begin{aligned}\left|1 - \frac{T_n}{S_n}\right| &\leq \frac{|S_{n_0-1} - T_{n_0-1}|}{S_n} + \varepsilon\left(1 - \frac{S_{n_0-1}}{S_n}\right) \\ &\leq \frac{|S_{n_0-1} - T_{n_0-1}|}{S_n} + \varepsilon.\end{aligned}$$

Tenant compte de $\lim\limits_{n\to+\infty} \frac{1}{S_n} = 0$, on en déduit qu'il existe un entier $n_1 \geq n_0$ tel que :

$$\forall n \geq n_1, \ \left|1 - \frac{T_n}{S_n}\right| \leq 2\varepsilon$$

ce qui traduit par $\lim\limits_{n\to+\infty} \frac{T_n}{S_n} = 1$, soit par l'équivalence de S_n et T_n quand n tend vers l'infini.

Remarque 1 *L'hypothèse x_n et y_n de mêmes signes (au moins à partir d'un certain rang) est essentielle dans le résultat précédent. Considérons par exemple la série de terme général $x_n = \frac{(-1)^n}{\sqrt{n} + (-1)^n}$. Un développement limité nous donne :*

$$\begin{aligned}x_n &= \frac{(-1)^n}{\sqrt{n}} \frac{1}{1 + \frac{(-1)^n}{\sqrt{n}}} = \frac{(-1)^n}{\sqrt{n}} - \frac{1}{n} + O\left(\frac{1}{n^{\frac{3}{2}}}\right) \\ &= \frac{(-1)^n}{\sqrt{n}} - \frac{1}{n} + r_n\end{aligned}$$

avec $|r_n| \leq \lambda \frac{1}{n^{\frac{3}{2}}}$, ce qui implique que la série de terme général x_n est divergente et pourtant x_n est équivalent $y_n = \frac{(-1)^n}{\sqrt{n}}$ qui est le terme général d'une série alternée convergente.

2.2 Résultat 2

1.

(a) Si on désigne par $S = \sum_{n=0}^{+\infty} u_n$ la somme la série de terme général u_n et par $(S_n)_{n\in\mathbb{N}}$ la suite de ses sommes partielles, alors pour tout $n \in \mathbb{N}$, la série $\sum_{k=n+1}^{+\infty} u_k$ est convergente et en notant v_n sa somme, on a :

$$v_n = S - S_n \underset{n\to+\infty}{\to} 0.$$

De plus avec $v_n = \sum_{k=n+1}^{+\infty} u_k = u_{n+1} + v_{n+1}$ et $u_{n+1} \geq 0$ pour tout $n \in \mathbb{N}$, on déduit que la suite $(v_n)_{n\in\mathbb{N}}$ est décroissante.

(b) On a :

$$\forall k \geq 1,\ u_k = v_{k-1} - v_k$$

et en utilisant le changement d'indice $j = k - 1$:

$$\begin{aligned}\sum_{k=1}^{n} ku_k &= \sum_{k=1}^{n} kv_{k-1} - \sum_{k=1}^{n} kv_k \\ &= \sum_{j=0}^{n-1} (j+1)\, v_j - \sum_{k=1}^{n} kv_k \\ &= \sum_{j=1}^{n-1} jv_j + \sum_{j=0}^{n-1} v_j - \sum_{k=1}^{n} kv_k \\ &= \sum_{j=0}^{n-1} v_j - nv_n.\end{aligned}$$

On peut aussi écrire, pour $n \geq 1$:

$$\sum_{k=0}^{n-1} v_k - nv_n = \sum_{k=0}^{n-1} (v_k - v_n)$$

avec :

$$v_k - v_n = \sum_{j=k+1}^{+\infty} u_j - \sum_{j=n+1}^{+\infty} u_j = \sum_{j=k+1}^{n} u_j$$

pour $0 \leq k \leq n-1$ et :

$$\begin{aligned}\sum_{k=0}^{n-1} (v_k - v_n) &= \sum_{j=1}^{n} u_j + \sum_{j=2}^{n} u_j + \cdots + \sum_{j=n}^{n} u_j \\ &= \sum_{j=1}^{n} \sum_{k=0}^{j-1} u_j = \sum_{j=1}^{n} j u_j.\end{aligned}$$

On peut aussi montrer le résultat par récurrence sur $n \geq 1$.
Pour $n = 1$, on a :

$$v_0 - v_1 = \sum_{k=1}^{+\infty} u_k - \sum_{k=2}^{+\infty} u_k = u_1$$

et supposant le résultat acquis au rang $n \geq 1$, on a :

$$\begin{aligned}\sum_{k=0}^{n} v_k - (n+1) v_{n+1} &= \sum_{k=0}^{n-1} v_k + v_n - (n+1) v_{n+1} \\ &= \sum_{k=0}^{n-1} v_k + v_n - (n+1)(v_n - u_{n+1}) \\ &= \sum_{k=0}^{n-1} v_k - n v_n + (n+1) u_{n+1} \\ &= \sum_{k=1}^{n} k u_k + (n+1) u_{n+1} = \sum_{k=1}^{n+1} k u_k.\end{aligned}$$

(c) En utilisant la positivité des v_n, on déduit de l'égalité précédente, que :

$$\forall n \geq 1,\ \sum_{k=1}^{n} k u_k \leq \sum_{k=0}^{n-1} v_k.$$

Si de plus la série $\sum v_n$ est convergente, on a :

$$\forall n \geq 1,\ U_n = \sum_{k=1}^{n} k u_k \leq V = \sum_{n=0}^{+\infty} v_n$$

et la suite croissante $(U_n)_{n \in \mathbb{N}}$ (les u_n sont tous positifs) est majorée, donc convergente vers un réel $U \leq V$. La série $\sum n u_n$ est donc convergente.

La suite $\left(\sum\limits_{k=n+1}^{+\infty} ku_k\right)_{n\in\mathbb{N}}$ des restes de cette série converge alors vers 0 et avec :

$$\forall n \geq 1,\ 0 \leq nv_n = n\sum_{k=n+1}^{+\infty} u_k \leq \sum_{k=n+1}^{+\infty} ku_k \underset{n\to+\infty}{\to} 0$$

on déduit que $\lim\limits_{n\to+\infty} nv_n = 0$ et $U = V$ compte tenu de **1.b**.

(d) C'est ce qu'on vient de montrer.

(e) On vient de montrer que si $\sum v_n$ converge alors $\sum nu_n$ converge vers la même limite.
Réciproquement si $\sum nu_n$ converge, on a alors $\lim\limits_{n\to+\infty} nv_n = 0$ (question **1.d.** ou **1.c.**) et avec :

$$\forall n \geq 1,\ V_n = \sum_{k=0}^{n-1} v_k = \sum_{k=1}^{n} ku_k + nv_n$$

on déduit que $\lim\limits_{n\to+\infty} V_n = \lim\limits_{n\to+\infty} \sum\limits_{k=1}^{n} ku_k$, soit que la série $\sum v_n$ converge et $\sum\limits_{n=0}^{+\infty} v_n = \sum\limits_{n=0}^{+\infty} nu_n$.
En définitive, ces deux séries sont ou bien convergentes de même somme, ou bien divergente vers l'infini.

2. En désignant par $(u_n)_{n\in\mathbb{N}}$ la suite réelle définie par :

$$\forall n \in \mathbb{N},\ u_n = \mathbb{P}(X = n)$$

on a :

$$\forall n \in \mathbb{N},\ \begin{cases} 0 \leq u_n \leq 1 \\ \sum\limits_{k=0}^{n} u_k = \sum\limits_{k=0}^{n} \mathbb{P}(X = k) = \mathbb{P}(X \leq n) \leq 1 \end{cases}$$

(on a $(X \leq n) = \bigcup\limits_{k=0}^{n} (X = k)$, les événements $(X = k)$ étant deux à deux incompatibles) c'est-à-dire que $\sum u_n$ est une série à termes positifs de sommes partielles bornées, elle est donc convergente et :

$$\forall n \in \mathbb{N},\ v_n = \sum_{k=n+1}^{+\infty} u_k = \sum_{k=n+1}^{+\infty} \mathbb{P}(X = k) = \mathbb{P}(X > n).$$

Si X admet une espérance $\mathbb{E}(X)$ alors $\mathbb{E}(X) = \sum\limits_{n=0}^{+\infty} n\mathbb{P}(X = n)$ et ce qui précède nous dit que $\mathbb{E}(X) = \sum\limits_{n=0}^{+\infty} v_n = \sum\limits_{n=0}^{+\infty} \mathbb{P}(X > n)$.
Réciproquement si $\sum \mathbb{P}(X > n) = \sum v_n$ converge, il en est de même de $\sum n\mathbb{P}(X = n)$ et ces deux séries ont même somme $\mathbb{E}(X)$.

Remarque 2 *Le résultat précédent peut aussi se montrer directement comme suit.*

1. *Pour tout entier naturel k, on note $p_k = \mathbb{P}(X = k)$ et pour tout entier naturel non nul k, on a :*

$$\begin{aligned}\mathbb{P}(X > k-1) - \mathbb{P}(X > k) &= \sum_{j=k}^{+\infty} \mathbb{P}(X = j) - \sum_{j=k+1}^{+\infty} \mathbb{P}(X = j) \\ &= \mathbb{P}(X = k) = p_k.\end{aligned}$$

2. *On en déduit que pour tout entier naturel non nul n, on a :*

$$\begin{aligned}\sum_{k=1}^{n} kp_k &= \sum_{k=1}^{n} k\mathbb{P}(X > k-1) - \sum_{k=1}^{n} k\mathbb{P}(X > k) \\ &= \sum_{k=0}^{n-1} (k+1)\mathbb{P}(X > k) - \sum_{k=1}^{n} k\mathbb{P}(X > k) \\ &= \sum_{k=0}^{n-1} \mathbb{P}(X > k) - n\mathbb{P}(X > n).\end{aligned}$$

3. *Si la variable aléatoire X admet une espérance $\mathbb{E}(X)$, avec la convergence de la série $\mathbb{E}(X) = \sum\limits_{k=0}^{+\infty} k\mathbb{P}(X = k)$, on a :*

$$0 \leq n\mathbb{P}(X > n) = n \sum_{k=n+1}^{+\infty} \mathbb{P}(X = k) \leq \sum_{k=n+1}^{+\infty} k\mathbb{P}(X = k) \underset{n\to+\infty}{\to} 0$$

donc $\lim\limits_{n\to+\infty} n\mathbb{P}(X > n) = 0$ et :

$$\sum_{k=0}^{n-1} \mathbb{P}(X > k) = \sum_{k=1}^{n} kp_k + n\mathbb{P}(X > n) \underset{n\to+\infty}{\to} \mathbb{E}(X) + 0,$$

soit :

$$\mathbb{E}(X) = \sum_{k=0}^{+\infty} \mathbb{P}(X > k).$$

4. Réciproquement si $\sum \mathbb{P}(X > k)$ converge, avec

$$\sum_{k=1}^{n} kp_k = \sum_{k=0}^{n-1} \mathbb{P}(X > k) - n\mathbb{P}(X > n) \leq \sum_{k=0}^{n-1} \mathbb{P}(X > k)$$

on déduit que $\sum k\mathbb{P}(X > k)$ converge et avec :

$$0 \leq n\mathbb{P}(X > n) \leq \sum_{k=n+1}^{+\infty} kp_k$$

on déduit que $\lim\limits_{n\to+\infty} n\mathbb{P}(X > n) = 0$ qui donne $\mathbb{E}(X) = \sum\limits_{k=0}^{+\infty} \mathbb{P}(X > k)$.

2.3 Résultat 3

1. La fonction f est définie et de classe $\mathcal{C}^\infty$ sur $]-R, R[$ comme toute somme d'une série entière de rayon R qui se respecte.
   De plus comme les coefficients a_n sont tous positifs ou nuls et les fonctions $x \mapsto x^n$ sont croissantes sur $\mathbb{R}^+$, la fonction f est croissante sur $[0, R[$ et en conséquence, elle a une limite finie en R si, et seulement si, elle majorée sur $[0, R[$. Dans le cas où elle n'est pas majorée, on a $\lim\limits_{x\to R^-} f(x) = +\infty$.
2.
   (a) Pour tout x dans $[0, R[$, on a compte tenu de la positivité des a_nR^n et de la croissance de f :

   $$\forall n \in \mathbb{N}, \sum_{k=0}^{n} a_k x^k \leq f(x) \leq L$$

   et faisant tendre x vers R, à n fixé, on en déduit que :

   $$S_n = \sum_{k=0}^{n} a_k R^k \leq L.$$

   (b) La majoration précédente nous dit que la suite croissante $(S_n)_{n\in\mathbb{N}}$ (les a_kR^k sont tous positifs) est majorée, elle est donc convergente de limite inférieure à L, ce qui signifie que $\sum\limits_{n=0}^{+\infty} a_nR^n \leq L$.

   (c) Pour tout $x \in [-R, R]$ et tout $n \in \mathbb{N}$, on a $|a_nx^n| \leq a_nR^n$, la série à termes positifs $\sum a_nR^n$ étant convergente. Il en résulte que la

série entière $\sum a_n x^n$ est normalement convergente sur $[-R, R]$. Sa somme f est alors continue sur $[-R, R]$ et :

$$L = \lim_{x \to R^-} f(x) = f(R) = \sum_{n=0}^{+\infty} a_n R^n.$$

3. Première modélisation : le cas particulier $N = 2$

1. On désigne par $J \in \{J_0, J_1\}$ le gagnant du premier jeu.
   Dire que le jeu s'arrête au rang $n = 2$ signifie que J gagne au deuxième jeu contre J_2.
   Dire que le jeu s'arrête au rang $n = 3$ signifie que J perd au deuxième jeu et que le gagnant J_2 de ce jeu va gagner au troisième jeu contre J_3.
   De manière générale, dire que le jeu s'arrête au rang $n > 2$ signifie que :
   - J perd contre J_2 au rang 2 ;
   - J_2 perd contre J_3 au rang 3 ;
   - $\cdots$;
   - le gagnant J_{n-1} du jeu numéro $n - 1$ gagne contre J_n au rang n.

   Avec les notations de l'énoncé, cela se traduit par :

   (a) $D_2 = \{(0, 0), (1, 1)\}$ pour $n = 2$;

   (b) $D_n = \{(0, 2, \cdots, n-2, n-1, n-1), (1, 2, \cdots, n-2, n-1, n-1)\}$ pour $n > 2$ ou encore

   $$D_{n+1} = \{(0, 2, \cdots, n-1, n, n), (1, 2, \cdots, n-1, n, n)\}$$

   pour $n \geq 2$.

2. On note $p \in]0, 1[$ la probabilité que J_1 soit le gagnant du premier jeu et $1 - p$ est la probabilité que ce soit J_0 le gagnant de ce jeu.
   Pour $n \geq 2$, on note $p_n \in]0, 1[$ la probabilité que le gagnant du jeu numéro n (s'il a lieu) soit J_n et $1 - p_n$ est la probabilité que le gagnant de ce jeu soit le joueur J_{n-1} dans le cas où $n > 2$ (c'est nécessairement lui qui est arrivé à ce stade) ou le joueur $J \in \{J_0, J_1\}$ du premier jeu pour $n = 2$.
   On peut utiliser un tableau pour schématiser ces possibilités. Su la première ligne figure la liste des joueurs et sur la première colonne la liste des duels. À l'intersection d'une ligne et d'une colonne on indique le gagnant avec sa probabilité de gagner. Pour $n = 2$, on a l'une des deux

possibilités suivantes :

	0	1
1		p
2		$1-p_2$

ou

	0	1
1	$1-p$	
2	$1-p_2$	

et pour $n=5$, dans le cas où J_0 gagne le premier duel, on a la situation suivante :

	0	1	2	3	4
1	$1-p$				
2			p_2		
3				p_3	
4					p_4
5					$1-p_5$

(a) On a :

$$\begin{aligned}\mathbb{P}(D_2) &= \mathbb{P}(0,0)+\mathbb{P}(1,1) = (1-p)(1-p_2)+p(1-p_2) \\ &= 1-p_2\end{aligned}$$

et pour $n \geq 3$:

$$\begin{aligned}\mathbb{P}(D_n) &= \mathbb{P}(0,2,\cdots,n-2,n-1,n-1)+(1,2,\cdots,n-2,n-1,n-1) \\ &= (1-p)\,p_2\cdots p_{n-2}p_{n-1}(1-p_n)+pp_2\cdots p_{n-2}p_{n-1}(1-p_n) \\ &= p_2\cdots p_{n-2}p_{n-1}(1-p_n)\end{aligned}$$

(deux épreuves consécutives $\mathcal{E}_{k-1}$ et $\mathcal{E}_k$, pour $k \geq 2$, sont indépendantes).
Dans le cas où la suite $(p_n)_{n\geq 2}$ est constante égale à p, on a $\mathbb{P}(D_2) = 1-p$ et $\mathbb{P}(D_n) = p^{n-2}(1-p)$ pour $n \geq 3$, soit :

$$\forall n \geq 2,\ \mathbb{P}(D_n) = p^{n-2}(1-p).$$

Les événements D_n étant deux à deux incompatibles, on a :

$$\begin{aligned}\mathbb{P}\left(\bigcup_{n=2}^{+\infty} D_n\right) &= \sum_{n=2}^{+\infty}\mathbb{P}(D_n) \\ &= (1-p)\sum_{n=2}^{+\infty}p^{n-2} = (1-p)\frac{1}{1-p} = 1.\end{aligned}$$

L'événement $D = \bigcup_{n\geq 2} D_n$ est la réalisation de l'un des D_n, ce qui signifie que le jeu va s'arrêter avec la probabilité 1.

(b) La variable aléatoire T est définie par $(T = n) = D_n$ pour $n \geq 2$ et $(T = 0) = (T = 1) = \emptyset$. Pour tout entier $n \geq 0$, on a :

$$\mathbb{P}(T > n) = \begin{cases} 1 \text{ si } n = 0 \text{ ou } n = 1 \\ 1 - \mathbb{P}(T \leq n) \text{ si } n \geq 2 \end{cases}$$

avec, pour $n \geq 2$:

$$\begin{aligned} \mathbb{P}(T \leq n) &= \sum_{k=2}^{n} \mathbb{P}(T = k) = \sum_{k=2}^{n} \mathbb{P}(D_k) \\ &= (1-p) \sum_{k=2}^{n} p^{k-2} = (1-p) \sum_{k=0}^{n-2} p^k = 1 - p^{n-1} \end{aligned}$$

ce qui donne :

$$\sum_{n=0}^{+\infty} \mathbb{P}(T > n) = 2 + \sum_{n=2}^{+\infty} p^{n-1} = 2 + p \sum_{n=0}^{+\infty} p^n = 2 + \frac{p}{1-p}.$$

Le résultat de la question **2.2.2.** nous dit alors que T admet une espérance donnée par :

$$\mathbb{E}(T) = \sum_{n=0}^{+\infty} \mathbb{P}(T > n) = 2 + \frac{p}{1-p} = \frac{2-p}{1-p}.$$

On peut aussi utiliser la formule classique pour l'espérance.
La série de terme général $n\mathbb{P}(T = n) = n\mathbb{P}(D_n)$ étant absolument convergente pour $p \in]0, 1[$ (critère de d'Alembert) on en déduit que T admet une espérance qui est donnée par :

$$\begin{aligned} \mathbb{E}(T) &= \sum_{n=1}^{+\infty} n\mathbb{P}(T = n) = (1-p) \sum_{n=2}^{+\infty} np^{n-2} \\ &= \frac{1-p}{p} \left(\sum_{n=1}^{+\infty} np^{n-1} - 1 \right) \\ &= \frac{1-p}{p} \left(\left(\sum_{n=0}^{+\infty} p^n \right)' - 1 \right) = \frac{1-p}{p} \left(\left(\frac{1}{1-p} \right)' - 1 \right) \\ &= \frac{1-p}{p} \left(\frac{1}{(1-p)^2} - 1 \right) = \frac{2-p}{1-p}. \end{aligned}$$

De même, La série de terme général $n^2\mathbb{P}(T=n)$ étant absolument convergente (critère de d'Alembert) on en déduit que T^2 admet une espérance qui est donnée par :

$$\begin{aligned}\mathbb{E}\left(T^2\right) &= \sum_{n=1}^{+\infty} n^2\mathbb{P}(T=n) = (1-p)\sum_{n=2}^{+\infty} n^2p^{n-2} \\ &= (1-p)\left(\sum_{n=2}^{+\infty} n(n-1)p^{n-2} + \sum_{n=2}^{+\infty} np^{n-2}\right) \\ &= (1-p)\left(\sum_{n=0}^{+\infty} p^n\right)'' + \mathbb{E}(T) \\ &= (1-p)\frac{2}{(1-p)^3} + \frac{2-p}{1-p} = \frac{p^2-3p+4}{(1-p)^2}.\end{aligned}$$

Il en résulte que T admet une variance donnée par :

$$\mathbb{V}(T) = \mathbb{E}\left(T^2\right) - (\mathbb{E}(T))^2 = \frac{p}{(1-p)^2}.$$

Les experts en probabilités auront remarqué que la variable aléatoire $X = T-1$ suit une loi géométrique de paramètre $1-p$ et il bien connu que $\mathbb{E}(X) = \dfrac{1}{1-p}$ et $\mathbb{V}(X) = \dfrac{p}{(1-p)^2}$, ce qui donne $\mathbb{E}(T) = \mathbb{E}(X)+1 = \dfrac{2-p}{1-p}$ et $\mathbb{V}(T) = \mathbb{V}(X) = \dfrac{p}{(1-p)^2}$ (on a de manière générale $\mathbb{E}(aX+b) = a\mathbb{E}(X)+b$ et $\mathbb{V}(aX+b) = a^2\mathbb{V}(X)$).

3. En **3.2.a.** on a vu que :

$$\mathbb{P}(D_n) = \begin{cases} 1-p_2 \text{ si } n=2 \\ p_2\cdots p_{n-2}p_{n-1}(1-p_n) \text{ si } n\geq 3\end{cases}$$

et en posant $\beta_n = \prod_{i=2}^{n} p_i$ pour $n\geq 2$, cela s'écrit :

$$\mathbb{P}(D_n) = \begin{cases} 1-\beta_2 \text{ si } n=2 \\ \beta_{n-1}-\beta_n \text{ si } n\geq 3\end{cases}$$

Il en résulte que pour $n\geq 2$, on a :

$$\mathbb{P}\left(\bigcup_{k=2}^{n} D_k\right) = \sum_{k=2}^{n}\mathbb{P}(D_k) = 1-\beta_n$$

(les D_k sont deux à deux incompatibles) et $\mathbb{P}\left(\bigcup\limits_{n=2}^{+\infty} D_n\right) = \sum\limits_{n=2}^{+\infty} \mathbb{P}(D_n) = 1$ (le jeu s'arrêtera sûrement) si, et seulement si, $\lim\limits_{n\to+\infty} \beta_n = 1$.

4. Dire que la suite de termes strictement positifs $(\beta_n)_{n\geq 2}$ converge vers 0 équivaut à dire que la suite $(\ln(\beta_n))_{n\geq 2} = \left(\sum\limits_{k=2}^{n} \ln(p_i)\right)_{n\geq 2}$ diverge vers $-\infty$, ce qui est encore équivalent à dire que la série de terme général positif $-\ln(p_n)$ est divergente. Dans le cas où $p_n = 1 - \dfrac{1}{n^\alpha}$ avec $\alpha > 0$, on a $-\ln(p_n) \underset{+\infty}{\backsim} \dfrac{1}{n^\alpha}$ avec $\sum \dfrac{1}{n^\alpha}$ qui diverge si, et seulement si, $\alpha \leq 1$. Il en résulte, d'après ce qui précède, que $\mathbb{P}\left(\bigcup\limits_{n=2}^{+\infty} D_n\right) = 1$ si, et seulement si, $\alpha \in]0, 1]$.

5. Pour $\alpha = 1$, on a

$$\forall n \geq 2,\ \beta_n = \prod_{i=2}^{n} p_i = \prod_{i=2}^{n} \frac{i-1}{i} = \frac{1}{n}$$

et la variable aléatoire T est à valeurs dans $\mathbb{N}$ avec :

$$\forall n \in \mathbb{N},\ \mathbb{P}(T = n) = \begin{cases} 0 \text{ si } n = 0 \text{ ou } n = 1 \\ \dfrac{1}{n(n-1)} = \text{ si } n \geq 2 \end{cases}$$

On a donc $n\mathbb{P}(T = n) = \dfrac{1}{n-1}$ pour $n \geq 2$ et $\sum\limits_{n=2}^{+\infty} n\mathbb{P}(T = n) = +\infty$, c'est-à-dire que la variable aléatoire T n'a pas d'espérance.

6.

(a) Pour tout réel $\alpha > 0$, les suites $(x_n)_{n\geq 2}$ et $(y_n)_{n\geq 2}$ définies par $x_n = -\ln(p_n) = -\ln\left(1 - \dfrac{1}{n^\alpha}\right)$ et $y_n = \dfrac{1}{n^\alpha}$ sont à termes positifs avec $x_n \underset{+\infty}{\sim} y_n$. De plus, pour $0 < \alpha < 1$ la série $\sum y_n$ diverge, il en est donc de même de $\sum x_n$ et les sommes partielles de ces séries sont équivalentes (question **2.1.**), c'est-à-dire que :

$$\sum_{k=2}^{n} -\ln(p_k) \underset{+\infty}{\sim} \sum_{k=2}^{n} \frac{1}{k^\alpha}.$$

(b) La fonction $t \to \dfrac{1}{t^\alpha}$ étant décroissante sur $\mathbb{R}^{+*}$, on a pour tout entier $k \geq 2$:

$$\frac{1}{k^\alpha} = \int_{k-1}^{k} \frac{dt}{k^\alpha} \leq \int_{k-1}^{k} \frac{dt}{t^\alpha} \leq \int_{k-1}^{k} \frac{dt}{(k-1)^\alpha} = \frac{1}{(k-1)^\alpha}$$

ce qui entraîne pour tout entier $n \geq 2$:

$$S_n = \sum_{k=2}^{n} \frac{1}{k^\alpha} \leq \sum_{k=2}^{n} \int_{k-1}^{k} \frac{dt}{t^\alpha} \leq \sum_{k=2}^{n} \frac{1}{(k-1)^\alpha}$$

avec :

$$\sum_{k=2}^{n} \int_{k-1}^{k} \frac{dt}{t^\alpha} = \int_{1}^{n} \frac{dt}{t^\alpha} = \frac{n^{1-\alpha}-1}{1-\alpha} \leq \frac{n^{1-\alpha}}{1-\alpha}$$

et :

$$\sum_{k=2}^{n} \frac{1}{(k-1)^\alpha} = 1 + S_n - \frac{1}{n^\alpha} \leq 1 + S_n.$$

On a donc :

$$S_n \leq \frac{n^{1-\alpha}}{1-\alpha} \leq \frac{1}{1-\alpha} + 1 + S_n = \beta + S_n$$

ou encore :

$$1 \leq \frac{1}{S_n}\frac{n^{1-\alpha}}{1-\alpha} \leq \frac{\beta}{S_n} + 1$$

avec $\lim\limits_{n\to+\infty} S_n = +\infty$ (la série $\sum \dfrac{1}{n^\alpha}$ diverge), ce qui entraîne $\lim\limits_{n\to+\infty} \dfrac{1}{S_n}\dfrac{n^{1-\alpha}}{1-\alpha} = 1$ ou encore $S_n = \sum\limits_{k=2}^{n} \dfrac{1}{k^\alpha} \underset{+\infty}{\sim} \dfrac{n^{1-\alpha}}{1-\alpha}$.

(c) Pour $n \geq 2$, on a :

$$u_n = \beta_n - \beta_{n+1} = \beta_n \left(1 - p_{n+1}\right) = \frac{\beta_n}{(n+1)^\alpha}$$

et pour tout réel $c > 0$:

$$\ln\left(n^c u_n\right) = \ln\left(\beta_n\right) + c\ln(n) - \alpha\ln(n+1)$$

avec :

$$-\ln\left(\beta_n\right) = -\sum_{k=2}^{n} \ln\left(p_k\right) \underset{+\infty}{\sim} \sum_{k=2}^{n} \frac{1}{k^\alpha} \underset{+\infty}{\sim} \frac{n^{1-\alpha}}{1-\alpha}$$

d'après les deux question précédentes. On a alors :

$$\frac{\ln(n)}{\ln(\beta_n)} \underset{+\infty}{\sim} -(1-\alpha)\frac{\ln(n)}{n^{1-\alpha}} \underset{n\to+\infty}{\to} 0$$

puisque $1-\alpha > 0$ et en conséquence :

$$\frac{\ln(n^c u_n)}{\ln(\beta_n)} = 1 + c\frac{\ln(n)}{\ln(\beta_n)} - \alpha\frac{\ln(n+1)}{\ln(\beta_n)} \underset{n\to+\infty}{\to} 1$$

ce qui signifie que :

$$\ln(n^c u_n) \underset{+\infty}{\sim} \ln(\beta_n) \underset{+\infty}{\sim} -\frac{n^{1-\alpha}}{1-\alpha}$$

et $\lim\limits_{n\to+\infty} \ln(n^c u_n) = -\infty$, encore équivalent à $\lim\limits_{n\to+\infty}(n^c u_n) = 0$.
Prenant $c = 3$, on aura $nu_n \leq \dfrac{1}{n^2}$ pour n assez grand, ce qui entraîne que la série à termes positifs $\sum nu_n$ est convergente.
En considérant que pour tout $n \geq 3$, on a :

$$n\mathbb{P}(T = n) = n(\beta_{n-1} - \beta_n) = nu_{n-1}$$

on en déduit que la série $\sum n\mathbb{P}(T = n)$ est convergente (nu_{n-1} est équivalent à $(n-1)u_{n-1}$), ce qui signifie que T admet une espérance.
On peut aussi écrire que pour tout $n \geq 2$, on a :

$$\mathbb{P}(T > n) = 1 - \mathbb{P}(T \leq n)$$

avec :

$$\mathbb{P}(T \leq n) = \sum_{k=2}^{n} \mathbb{P}(D_k) = \mathbb{P}\left(\bigcup_{k=2}^{n} D_k\right) = 1 - \beta_n$$

ce qui donne :

$$\mathbb{P}(T > n) = \beta_n.$$

Puis avec :

$$\frac{\ln(n^2\beta_n)}{\ln(\beta_n)} = 1 + 2\frac{\ln(n)}{\ln(\beta_n)}$$

et $\ln(\beta_n) \underset{+\infty}{\sim} -\dfrac{n^{1-\alpha}}{1-\alpha}$, on déduit que $\lim\limits_{n\to+\infty} \dfrac{\ln(n^2\beta_n)}{\ln(\beta_n)} = 1$, soit $\ln(n^2\beta_n) \underset{+\infty}{\sim} \ln(\beta_n) \underset{+\infty}{\sim} -\dfrac{n^{1-\alpha}}{1-\alpha}$ qui entraîne $\lim\limits_{n\to+\infty}(n^2\beta_n) = 0$ et la convergence de $\sum \beta_n$. Il en résulte T admet une espérance (question **2.2.2.**).

4. Deuxième modélisation : le cas où les probabilités sont constantes

4.1. Cas particulier : $N = 3$ et $p = \frac{1}{2}$

1. Dire que J_n est vainqueur du tournoi signifie que J_n a participé aux trois duels $\mathcal{E}_n$, $\mathcal{E}_{n+1}$ et $\mathcal{E}_{n+2}$ en remportant chacun de ces duels, ce qui se traduit par :

$$\forall n \in \mathbb{N},\ \mathbb{P}(G_n) = \mathbb{P}(A_n)\, p_n\,(1 - p_{n+1})\,(1 - p_{n+2})$$

(les duels sont indépendants et A_n ne dépend que des duels $\mathcal{E}_k$ pour $k \leq n-1$). Dans le cas où $p_n = p = \frac{1}{2}$, on a :

$$\forall n \in \mathbb{N},\ \mathbb{P}(G_n) = \mathbb{P}(A_n)\, p\,(1-p)^2 = \frac{1}{8}\mathbb{P}(A_n)$$

2. Comme il faut remporter trois duels consécutifs pour être le vainqueur, les événements A_0, A_1, A_2 et A_3 sont quasi-certains, c'est-à-dire de probabilité égale à 1 (l'événement Ω est l'événement certain, mais en général $\mathbb{P}(A) = 1$ n'entraîne pas $A = \Omega$, on dit plutôt que si $\mathbb{P}(A) = 1$ alors A est quasi-certain).

3.

   (a) Si pour $3 \leq k \leq n-1$ (avec $n \geq 4$) l'événement $A_{n,k}$ est réalisé, alors J_{n-k} est arrivé au duel numéro n et en conséquence il a remporté les duels $n-k, n-k+1, \cdots, n-1$, soit un total de $k \geq 3$ duels successifs, ce qui n'est pas possible pour $N = 3$. On a donc $\mathbb{P}(A_{n,k}) = 0$ pour $3 \leq k \leq n-1$ et en écrivant que $A_n = \bigcup_{k=1}^{n-1} A_{n,k}$, les événements $A_{n,k}$ étant deux à deux incompatibles, on a :

$$\forall n \geq 4,\ \mathbb{P}(A_n) = \sum_{k=1}^{n-1} \mathbb{P}(A_{n,k}) = \mathbb{P}(A_{n,1}) + \mathbb{P}(A_{n,2})\,.$$

   L'événement $A_{n,1}$ se traduit par : A_{n-1} est réalisé (J_{n-1} participe aux duels $n-1$ et n) et J_{n-1} a remporté le duel $n-1$, ce qui donne :

$$\mathbb{P}(A_{n,1}) = \mathbb{P}(A_{n-1})\, p_{n-1} = \mathbb{P}(A_{n-1})\, p = \frac{1}{2}\mathbb{P}(A_{n-1})\,.$$

De même, l'événement $A_{n,2}$ se traduit par : A_{n-2} est réalisé (J_{n-2} participe aux duels $n-2, n-1$ et n) et J_{n-2} a remporté les duels $n-2$ et $n-1$, ce qui donne :

$$\begin{aligned}\mathbb{P}(A_{n,2}) &= \mathbb{P}(A_{n-2})\, p_{n-2}(1-p_{n-1}) \\ &= \mathbb{P}(A_{n-2})\, p(1-p) = \frac{1}{4}\mathbb{P}(A_{n-2}).\end{aligned}$$

On a donc la relation de récurrence :

$$\forall n \geq 4,\ \mathbb{P}(A_n) = \frac{1}{2}\mathbb{P}(A_{n-1}) + \frac{1}{4}\mathbb{P}(A_{n-2}).$$

(b) On définit la suite réelle $(u_n)_{n\in\mathbb{N}}$ par $u_n = \mathbb{P}(A_{n+2})$ pour tout $n \in \mathbb{N}$. Cette suite vérifie la relation de récurrence :

$$\begin{cases} u_0 = \mathbb{P}(A_2) = 1,\ u_1 = \mathbb{P}(A_3) = 1 \\ \forall n \geq 2,\ u_n - \frac{1}{2}u_{n-1} - \frac{1}{4}u_{n-2} = 0 \end{cases}$$

et on sait que l'ensemble E de ces suites est un espace vectoriel réel de dimension 2, ce qui se justifie en remarquant l'application :

$$\begin{array}{rccc} \varphi : & E & \rightarrow & \mathbb{R}^2 \\ & (u_n)_{n\in\mathbb{N}} & \mapsto & (u_0, u_1) \end{array}$$

est un isomorphisme (un élément de E est uniquement déterminé par ses valeurs initiales u_0 et u_1).
L'équation caractéristique de cette récurrence, $r^2 - \frac{1}{2}r - \frac{1}{4} = 0$, ayant deux racines réelles $r_1 = \frac{1}{4}\left(1-\sqrt{5}\right)$ et $r_2 = \frac{1}{4}\left(1+\sqrt{5}\right)$, on déduit que les suites $(r_1^n)_{n\in\mathbb{N}}$ et $(r_2^n)_{n\in\mathbb{N}}$ forment une base de E et pour toute suite $(u_n)_{n\in\mathbb{N}}$ dans E il existe deux constantes réelles α et β uniquement déterminées telles que $u_n = \alpha r_1^n + \beta r_2^n$ pour tout $n \in \mathbb{N}$.
On a donc :

$$\forall n \in \mathbb{N},\ \mathbb{P}(A_{n+2}) = \alpha r_1^n + \beta r_2^n$$

ou encore :

$$\forall n \geq 2,\ \mathbb{P}(A_n) = \alpha r_1^{n-2} + \beta r_2^{n-2}.$$

les constantes α et β étant solutions du système :

$$\begin{cases} \alpha + \beta = \mathbb{P}(A_2) = 1 \\ \alpha r_1 + \beta r_2 = \mathbb{P}(A_3) = 1 \end{cases}$$

soit :

$$\left\{\begin{array}{l} \alpha+\beta=1 \\ \left(1-\sqrt{5}\right)\alpha+\left(1+\sqrt{5}\right)\beta=4 \end{array}\right.$$

ou encore :

$$\left\{\begin{array}{l} \alpha+\beta=1 \\ \beta-\alpha=\dfrac{3}{\sqrt{5}} \end{array}\right.$$

ce qui donne :

$$\left\{\begin{array}{l} \alpha=\dfrac{\sqrt{5}-3}{2\sqrt{5}} \\ \beta=\dfrac{\sqrt{5}+3}{2\sqrt{5}} \end{array}\right.$$

Tenant compte du fait que r_1 et r_2 sont racines de $r^2=\dfrac{1}{4}(2r+1)$, on a :

$$\left\{\begin{array}{l} r_1^2=\dfrac{3-\sqrt{5}}{8} \\ r_2^2=\dfrac{3+\sqrt{5}}{8} \end{array}\right. \text{ et } \left\{\begin{array}{l} \dfrac{\alpha}{r_1{}^2}=-\dfrac{4}{\sqrt{5}} \\ \dfrac{\beta}{r_2^2}=\dfrac{4}{\sqrt{5}} \end{array}\right.$$

On a donc en définitive :

$$\forall n\geq 2,\ \mathbb{P}(A_n)=\frac{\alpha}{r_1{}^2}r_1^n+\frac{\beta}{r_2^2}r_2^n=\frac{4}{\sqrt{5}}\left(r_2^n-r_1^n\right).$$

(c) Le jeu s'arrête s'il y a un gagnant, donc la probabilité que le jeu s'arrête est donnée par :

$$P=\mathbb{P}\left(\bigcup_{n=0}^{+\infty}G_n\right)=\sum_{n=0}^{+\infty}\mathbb{P}(G_n)=\frac{1}{8}\sum_{n=0}^{+\infty}\mathbb{P}(A_n)$$

(les G_n sont deux à deux incompatibles). Tenant compte de $\mathbb{P}(A_0)=\mathbb{P}(A_1)=1$ et de la formule donnant les $\mathbb{P}(A_n)$ pour $n\geq 2$, on a :

$$P=\frac{1}{4}+\frac{1}{2\sqrt{5}}\left(\sum_{n=2}^{+\infty}r_2^n-\sum_{n=2}^{+\infty}r_1^n\right).$$

En remarquant que $r_2-r_1=\dfrac{\sqrt{5}}{2}$, on a :

$$P=\frac{1}{2\sqrt{5}}\left(\sum_{n=1}^{+\infty}r_2^n-\sum_{n=1}^{+\infty}r_1^n\right)$$

avec :

$$\sum_{n=1}^{+\infty} r_j^n = \frac{1}{1-r_j} - 1 \ (j = 1, 2)$$

ce qui donne :

$$\begin{aligned} P &= \frac{1}{2\sqrt{5}} \left(\frac{1}{1-r_2} - \frac{1}{1-r_1} \right) \\ &= \frac{1}{2\sqrt{5}} \frac{r_2 - r_1}{(1-r_2)(1-r_1)} \end{aligned}$$

avec

$$\begin{cases} r_1 + r_2 = \frac{1}{2}, \ r_1 r_2 = -\frac{1}{4} \\ (1-r_2)(1-r_1) = 1 - (r_1 + r_2) + r_1 r_2 = \frac{1}{4} \end{cases}$$

On a donc :

$$P = \frac{1}{2\sqrt{5}} \frac{\sqrt{5}}{2} 4 = 1.$$

(d) La loi de la variable aléatoire T égale au nombre de duels pour que le jeu s'arrête est donnée par $T(\Omega) = \mathbb{N}$ avec $\mathbb{P}(T = n) = 0$ pour $n = 0, 1, 2$ (il faut remporter au moins trois duels). L'événement $(T = 3)$ est réalisé si J_0 ou J_1 gagne, donc :

$$\mathbb{P}(T = 3) = \mathbb{P}(G_0) + \mathbb{P}(G_1) = \frac{1}{8} (\mathbb{P}(A_0) + \mathbb{P}(A_1)) = \frac{1}{4}$$

et pour $n \geq 4$, $(T = n)$ signifie que J_{n-2} a remporté trois duels consécutifs, donc :

$$\mathbb{P}(T = n) = \mathbb{P}(G_{n-2}) = \frac{1}{8} \mathbb{P}(A_{n-2}) = \frac{1}{2\sqrt{5}} \left(r_2^{n-2} - r_1^{n-2} \right).$$

On peut remarquer que cette formule est aussi valable pour $n = 3$ $(r_2 - r_1 = \frac{\sqrt{5}}{2})$.

(e) La série $\sum n\mathbb{P}(T = n)$ est convergente (différence de deux séries géométriques convergentes), donc T admet une espérance donnée

par :

$$\begin{aligned}
\mathbb{E}(T) &= \frac{1}{2\sqrt{5}}\sum_{n=3}^{+\infty} n\left(r_2^{n-2}-r_1^{n-2}\right) = \frac{1}{2\sqrt{5}}\sum_{n=1}^{+\infty}(n+2)\left(r_2^n-r_1^n\right)\\
&= \frac{1}{2\sqrt{5}}\sum_{n=1}^{+\infty} n\left(r_2^n-r_1^n\right) + \frac{2}{2\sqrt{5}}\sum_{n=1}^{+\infty}\left(r_2^n-r_1^n\right)\\
&= \frac{1}{2\sqrt{5}}\sum_{n=1}^{+\infty} n\left(r_2^n-r_1^n\right) + 2
\end{aligned}$$

(voir le calcul qui précède) avec, pour $0 < r < 1$:

$$\sum_{n=1}^{+\infty} nr^n = r\sum_{n=1}^{+\infty} nr^{n-1} = \frac{r}{(1-r)^2}$$

ce qui donne :

$$\begin{aligned}
\mathbb{E}(T) &= 2 + \frac{1}{2\sqrt{5}}\left(\frac{r_2}{(1-r_2)^2} - \frac{r_1}{(1-r_1)^2}\right)\\
&= 2 + \frac{1}{2\sqrt{5}}\frac{r_2(1-r_1)^2 - r_1(1-r_2)^2}{(1-r_1)^2(1-r_2)^2}
\end{aligned}$$

avec $r_2 - r_1 = \dfrac{\sqrt{5}}{2}$, $r_1 + r_2 = \dfrac{1}{2}$, $r_1r_2 = -\dfrac{1}{4}$, $(1-r_2)(1-r_1) = \dfrac{1}{4}$ et

$$\begin{aligned}
r_2(1-r_1)^2 - r_1(1-r_2)^2 &= r_2 - r_1 + r_1r_2(r_1-r_2)\\
&= (r_2-r_1)(1-r_1r_2) = \frac{\sqrt{5}}{2}\frac{5}{4}
\end{aligned}$$

ce qui donne :

$$\mathbb{E}(T) = 2 + \frac{1}{2\sqrt{5}}\frac{\frac{\sqrt{5}}{2}\frac{5}{4}}{\frac{1}{16}} = 7.$$

4.2. Étude du cas général

1.

(a) Dire que J_0 est vainqueur du tournoi revient à dire qu'il remporte les duels 1 à N, donc :

$$g_0 = \mathbb{P}(G_0) = (1-p)(1-p_2)\cdots(1-p_N) = (1-p)^N.$$

De même, on a :

$$g_1 = \mathbb{P}(G_1) = p(1-p_2)\cdots(1-p_N) = p(1-p)^{N-1}.$$

Comme il faut remporter N duels consécutifs pour être le vainqueur, les J_k pour $0 \leq k \leq N$ participent tous au tournoi, ce qui signifie que :

$$a_k = \mathbb{P}(A_k) = 1 \ \ (0 \leq k \leq N)$$

(b) Pour tout entier naturel n, on a :

$$\begin{cases} 0 \leq g_n = \mathbb{P}(G_n) \leq 1 \\ \sum\limits_{k=0}^{n} g_k = \sum\limits_{k=0}^{n} \mathbb{P}(G_k) = \mathbb{P}\left(\bigcup\limits_{k=0}^{n} G_k\right) \leq 1 \end{cases}$$

(les événements G_k étant deux à deux incompatibles) c'est-à-dire que $\sum g_n$ est une série à termes positifs de sommes partielles bornées, elle est donc convergente.

(c) Dire que, pour $n \geq 1$, J_n est vainqueur du tournoi revient à dire qu'il participe aux N duels $\mathcal{E}_n, \cdots, \mathcal{E}_{n+N-1}$ et les remporte, donc :

$$\begin{aligned} g_n = \mathbb{P}(G_n) &= \mathbb{P}(A_n)\, p_n (1-p_{n+1})\cdots(1-p_{n+N-1}) \\ &= a_n p(1-p)^{N-1}. \end{aligned}$$

La convergence de la série $\sum a_n$ se déduit alors de celle de $\sum g_n$ et on a :

$$S = \sum_{n=1}^{+\infty} a_n = \frac{1}{p(1-p)^{N-1}} \sum_{n=1}^{+\infty} g_n.$$

2.

(a) Comme en **4.1.3.a.** on vérifie que $\mathbb{P}(A_{n,k}) = 0$ pour $N \leq k \leq n-1$ puisque un joueur qui remporte N duels successifs est gagnant et provoque l'arrêt du tournoi. On a alors pour $n \geq N+1$:

$$\mathbb{P}(A_n) = \mathbb{P}\left(\bigcup_{k=1}^{n-1} A_{n,k}\right) = \mathbb{P}\left(\bigcup_{k=1}^{N-1} A_{n,k}\right) = \sum_{k=1}^{N-1} \mathbb{P}(A_{n,k}).$$

Pour $1 \leq k \leq N-1$, l'événement $A_{n,k}$ se traduit par : A_{n-k} est réalisé (J_{n-k} participe aux duels $n-k$ à n) et J_{n-k} a remporté le duel $n-k$ à $n-1$, ce qui donne :

$$\begin{aligned} \mathbb{P}(A_{n,k}) &= \mathbb{P}(A_{n-k})\, p_{n-k}(1-p_{n-k+1})\cdots(1-p_{n-1}) \\ &= a_{n-k}\, p(1-p)^{k-1}. \end{aligned}$$

On a donc la relation de récurrence d'ordre $N-1$:

$$\forall n \geq N+1,\ a_n = \mathbb{P}(A_n) = p \sum_{k=1}^{N-1} a_{n-k} (1-p)^{k-1}.$$

Pour $n = N+1$, on a :

$$\begin{aligned}(a_{n-k})_{1\leq k \leq N-1} &= (a_{N+1-k})_{1\leq k\leq N-1} \\ &= (a_N, a_{N-1}, \cdots, a_2) = (1, 1, \cdots, 1)\end{aligned}$$

et :

$$\begin{aligned}a_{N+1} &= p \sum_{k=1}^{N-1} (1-p)^{k-1} = p \sum_{j=0}^{N-2} (1-p)^j \\ &= p \frac{1-(1-p)^{N-1}}{1-(1-p)} = 1-(1-p)^{N-1}.\end{aligned}$$

(b) Comme $a_n = 1$ pour $1 \leq n \leq N$, on a :

$$S = N + \sum_{n=N+1}^{+\infty} a_n = N + R_N$$

et avec ce qui précède :

$$\begin{aligned}R_N &= p \sum_{n=N+1}^{+\infty} \sum_{k=1}^{N-1} a_{n-k} (1-p)^{k-1} \\ &= p \sum_{k=1}^{N-1} (1-p)^{k-1} \sum_{n=N+1}^{+\infty} a_{n-k}\end{aligned}$$

avec, pour tout k compris entre 1 et $N-1$:

$$\begin{aligned}\sum_{n=N+1}^{+\infty} a_{n-k} &= a_{N+1-k} + a_{N+2-k} + \cdots = \sum_{j=N-k+1}^{+\infty} a_j \\ &= S - \sum_{j=1}^{N-k} a_j = S - \sum_{i=k}^{N-1} a_{N-i}\end{aligned}$$

(on a posé $i = N - j$ dans la dernière somme). On a donc :

$$\begin{aligned} R_N &= p \sum_{k=1}^{N-1} (1-p)^{k-1} \left(S - \sum_{i=k}^{N-1} a_{N-i} \right) \\ &= pS \sum_{k=1}^{N-1} (1-p)^{k-1} - p \sum_{k=1}^{N-1} (1-p)^{k-1} \sum_{i=k}^{N-1} a_{N-i} \\ &= S \left(1 - (1-p)^{N-1} \right) - p \sum_{k=1}^{N-1} (1-p)^{k-1} \sum_{i=k}^{N-1} a_{N-i} \end{aligned}$$

et :

$$S = N + S \left(1 - (1-p)^{N-1} \right) - p \sum_{k=1}^{N-1} (1-p)^{k-1} \sum_{i=k}^{N-1} a_{N-i}$$

ou encore :

$$\begin{aligned} (1-p)^{N-1} S &= N - p \sum_{k=1}^{N-1} (1-p)^{k-1} \sum_{i=k}^{N-1} a_{N-i} \\ &= N - p \sum_{1 \le k \le i \le N-1} (1-p)^{k-1} a_{N-i}. \end{aligned}$$

En écrivant que :

$$\begin{aligned} \sum_{1 \le k \le i \le N-1} (1-p)^{k-1} a_{N-i} &= \sum_{i=1}^{N-1} \sum_{k=1}^{i} (1-p)^{k-1} a_{N-i} \\ &= \sum_{i=1}^{N-1} a_{N-i} \sum_{k=1}^{i} (1-p)^{k-1} \\ &= \sum_{i=1}^{N-1} a_{N-i} \sum_{j=0}^{i-1} (1-p)^{j} \\ &= \sum_{i=1}^{N-1} a_{N-i} \frac{1-(1-p)^i}{p} \end{aligned}$$

on déduit que :

$$(1-p)^{N-1} S = N - \sum_{i=1}^{N-1} a_{N-i} \left(1 - (1-p)^i \right)$$

avec $a_{N-i} = 1$ pou $1 \leq i \leq N-1$, ce qui donne :

$$\begin{aligned}
(1-p)^{N-1} S &= N - \sum_{i=1}^{N-1} \left(1 - (1-p)^i\right) \\
&= N - (N-1) + (1-p) \sum_{i=1}^{N-1} (1-p)^{i-1} \\
&= 1 + (1-p) \sum_{j=0}^{N-2} (1-p)^j \\
&= 1 + (1-p) \frac{1-(1-p)^{N-1}}{p} \\
&= \frac{1-(1-p)^{N-1}}{p} + (1-p)^{N-1}.
\end{aligned}$$

On a donc en définitive :

$$\begin{aligned}
S = \sum_{n=1}^{+\infty} a_n &= \frac{1}{p(1-p)^{N-1}} \sum_{n=1}^{+\infty} g_n \\
&= \frac{1-(1-p)^{N-1}}{p(1-p)^{N-1}} + 1 = \frac{1-(1-p)^N}{p(1-p)^{N-1}}
\end{aligned}$$

et :

$$\sum_{n=0}^{+\infty} g_n = g_0 + \sum_{n=1}^{+\infty} g_n = (1-p)^N + 1 - (1-p)^N = 1,$$

ce qui signifie que le jeu se terminera avec la probabilité 1.

3.

(a) La loi de la variable aléatoire T égale au nombre de duels pour que le jeu s'arrête est donnée par $T(\Omega) = \mathbb{N}$ avec $\mathbb{P}(T = n) = 0$ pour $0 \leq n \leq N-1$ puisqu'il faut remporter au moins N duels pour être vainqueur.
L'événement $(T = N)$ est réalisé si J_0 ou J_1 est vainqueur du tournoi, donc :

$$\begin{aligned}
\mathbb{P}(T = N) &= \mathbb{P}(G_0) + \mathbb{P}(G_1) = g_0 + g_1 \\
&= (1-p)^N + p(1-p)^{N-1} = (1-p)^{N-1}.
\end{aligned}$$

Pour $n \geq N+1$, $(T = n)$ signifie que J_{n-N+1} a remporté N duels consécutifs, donc :

$$\begin{aligned}\mathbb{P}(T = n) &= \mathbb{P}(G_{n-N+1}) = g_{n-N+1} \\ &= a_{n-N+1} p (1-p)^{N-1}.\end{aligned}$$

On a donc, pour tout entier naturel n :

$$\mathbb{P}(T = n) = \begin{cases} 0 \text{ si } 0 \leq n \leq N-1 \\ (1-p)^{N-1} \text{ si } n = N+1 \\ g_{n-N+1} = a_{n-N+1} p (1-p)^{N-1} \text{ si } n \geq N+1 \end{cases}$$

ou encore :

$$g_m = \begin{cases} (1-p)^N \text{ si } m = 0 \\ p(1-p)^{N-1} = \mathbb{P}(T = N) - g_0 \text{ si } m = 1 \\ \mathbb{P}(T = m+N-1) \text{ si } m \geq 2 \end{cases}$$

(on a posé $m = n - N + 1$ pour $n \geq N+1$) et $a_m = \dfrac{g_m}{p(1-p)^{N-1}}$ pour $m \geq 1$.

Pour $n \geq 1$, dire que A_n est réalisé signifie que J_n participe à un duel, ce qui équivaut à $T \geq n$, on a donc :

$$\forall n \geq 1,\ a_n = \mathbb{P}(T \geq n).$$

(b) La série $\sum a_n$ étant convergente, il en est de même de $\sum \mathbb{P}(T \geq n)$ ou de $\sum \mathbb{P}(T > n)$, il en résulte que T admet une espérance donnée par :

$$\begin{aligned}\mathbb{E}(T) &= \sum_{n=0}^{+\infty} \mathbb{P}(T > n) = \sum_{n=0}^{+\infty} a_{n+1} \\ &= S = \frac{1-(1-p)^N}{p(1-p)^{N-1}}.\end{aligned}$$

Pour $N = 3$ et $p = \dfrac{1}{2}$, on retrouve :

$$\mathbb{E}(T) = \frac{1 - \frac{1}{8}}{\frac{1}{2}\frac{1}{4}} = 7.$$

Pour $N = 2$ et $0 < p < 1$, on a :

$$\mathbb{E}(T) = \frac{2-p}{1-p}.$$

Pour $N \geq 2$ et $p = \frac{1}{2}$, on a :

$$\mathbb{E}(T) = 2^N - 1 \underset{N \to +\infty}{\to} +\infty.$$

(c) Pour $n \geq N+1$, on a :

$$\begin{aligned} a_n - a_{n+1} &= \mathbb{P}(T \geq n) - \mathbb{P}(T \geq n+1) \\ &= \mathbb{P}(T = n) = g_{n-N+1} = a_{n-N+1} p (1-p)^{N-1}. \end{aligned}$$

Pour $n = N$, on a $a_N = 1$, $a_{N+1} = 1-(1-p)^{N-1}$, $a_{n-N+1} = a_1 = 1$ et :

$$a_N - a_{N+1} = a_1 (1-p)^{N-1}.$$

5. Comportement asymptotique de la loi de T

5.1. Un lemme

Chaque nombre complexe non nul z_k $(1 \leq k \leq r)$ peut s'écrire $z_k = \rho_k e^{i\theta_k}$ avec $\rho_k = |z_k| > 0$ et $\theta_k \in \left]-\pi, \pi\right]$. On a alors :

$$\begin{cases} \left|\sum\limits_{k=1}^{r} z_k\right|^2 = \sum\limits_{k=1}^{r} |z_k|^2 + 2 \sum\limits_{1 \leq j < k \leq r} \rho_j \rho_k \cos(\theta_j - \theta_k), \\ \left(\sum\limits_{k=1}^{r} |z_k|\right)^2 = \sum\limits_{k=1}^{r} |z_k|^2 + 2 \sum\limits_{1 \leq j < k \leq n} \rho_j \rho_k \end{cases}$$

et l'égalité $\left|\sum\limits_{k=1}^{r} z_k\right| = \sum\limits_{k=1}^{r} |z_k|$ est équivalente à :

$$\sum_{1 \leq j < k \leq r} \rho_j \rho_k (1 - \cos(\theta_j - \theta_k)) = 0.$$

Tous les termes de cette somme étant positifs ou nuls avec $\rho_j \rho_k > 0$, on en déduit que $\cos(\theta_j - \theta_k) = 1$ avec $\theta_j - \theta_k \in \left]-2\pi, 2\pi\right[$ pour $1 \leq j < k \leq r$ (on a $-\pi < \theta_j \leq \pi$ et $-\pi < \theta_k \leq \pi$ donc $-\pi \leq -\theta_k < \pi$ et $-2\pi < \theta_j - \theta_k < 2\pi$),

ce qui donne $\theta_j = \theta_k$ et en notant θ cette valeur commune on a $z_k = \rho_k e^{i\theta} = |z_k| e^{i\theta}$ pour tout entier k compris entre 1 et r ou encore :

$$z_k = \frac{|z_k|}{|z_1|} |z_1| e^{i\theta} = \lambda_k z_1 \ \ (1 \leq k \leq r)$$

où on a posé $\lambda_k = \dfrac{|z_k|}{|z_1|}$ pour tout k compris entre 1 et r.

Réciproquement si $z_k = \lambda_k z_1$ avec $\lambda_k > 0$ pour tout k compris entre 2 et r et $\lambda_1 = 1$, on a :

$$\left| \sum_{k=1}^{r} z_k \right| = |z_1| \sum_{k=1}^{r} \lambda_k = \sum_{k=1}^{r} \lambda_k |z_1| = \sum_{k=1}^{r} |z_k| .$$

On peut aussi démontrer ce résultat par récurrence sur $r \geq 1$, le cas $r = 2$ correspondant au cas d'égalité dans l'inégalité triangulaire sur $\mathbb{C}$.

5.2. Étude d'une fonction associée à T

1. La variable aléatoire T étant à valeurs dans $\mathbb{N}$ et admettant une espérance, on sait que la série $\sum \mathbb{P}(T > n)$ est convergente de somme $\mathbb{E}(T)$. Il en résulte que la série entière $\sum \mathbb{P}(T > n) x^n$ est normalement convergente sur l'intervalle $[-1, 1]$ et sa somme $Q(x) = \sum\limits_{n=0}^{+\infty} \mathbb{P}(T > n) x^n$ est continue sur $[-1, 1]$. La théorie des séries entières nous dit que le rayon de convergence de cette série est $R \geq 1$ et sa somme est $\mathcal{C}^\infty$ sur $]-R, R[$, donc sur $]-1, 1[$.

2. Pour $x \in]-1, 1[$, on a :

$$\begin{aligned} Q(x) &= \sum_{n=0}^{+\infty} \mathbb{P}(T > n) x^n = \sum_{n=0}^{+\infty} \mathbb{P}(T \geq n+1) x^n \\ &= \sum_{n=0}^{+\infty} a_{n+1} x^n = \sum_{n=0}^{N-1} a_{n+1} x^n + R(x) \end{aligned}$$

et en tenant compte de **4.2.3.c.** on a :

$$\begin{aligned} xR(x) &= \sum_{n=N}^{+\infty} a_{n+1}x^{n+1} = \sum_{n=N+1}^{+\infty} a_n x^n \\ &= \sum_{n=N+1}^{+\infty} \left(a_{n+1} + a_{n-N+1}p(1-p)^{N-1}\right) x^n \\ &= \sum_{n=N+1}^{+\infty} a_{n+1}x^n + p(1-p)^{N-1} \sum_{n=N+1}^{+\infty} a_{n-N+1}x^n \\ &= \sum_{n=N+1}^{+\infty} a_{n+1}x^n + p(1-p)^{N-1} x^N \sum_{n=1}^{+\infty} a_{n+1}x^n \end{aligned}$$

ce qui donne :

$$\begin{aligned} xQ(x) &= \sum_{n=0}^{N-1} a_{n+1}x^{n+1} + xR(x) \\ &= \sum_{n=0}^{N-1} a_{n+1}x^{n+1} + \sum_{n=N+1}^{+\infty} a_{n+1}x^n + p(1-p)^{N-1} x^N \sum_{n=1}^{+\infty} a_{n+1}x^n. \end{aligned}$$

Comme par ailleurs $a_n = 1$ pour $0 \leq n \leq N$, on peut écrire que :

$$\sum_{n=0}^{N-1} a_{n+1}x^{n+1} = \sum_{n=0}^{N-1} x^{n+1} = \sum_{n=1}^{N} x^n = \sum_{n=1}^{N-1} a_{n+1}x^n + x^N$$

et :

$$\begin{aligned} xQ(x) &= \sum_{n=1}^{N-1} a_{n+1}x^n + x^N + \sum_{n=N+1}^{+\infty} a_{n+1}x^n + p(1-p)^{N-1} x^N (Q(x) - 1) \\ &= Q(x) - 1 + (1 - a_{N+1}) x^N + p(1-p)^{N-1} x^N (Q(x) - 1) \\ &= Q(x)\left(1 + p(1-p)^{N-1} x^N\right) - 1 + (1 - a_{N+1}) x^N - p(1-p)^{N-1} x^N \end{aligned}$$

avec $1 - a_{N+1} = (1-p)^{N-1}$, ce qui donne :

$$xQ(x) = Q(x)\left(1 + p(1-p)^{N-1} x^N\right) - 1 + (1-p)^N x^N$$

ou encore :

$$Q(x)\left(1 - x + p(1-p)^{N-1} x^N\right) = 1 - (1-p)^N x^N$$

qui peut aussi s'écrire :

$$Q(x)\left(1-x+\frac{p}{1-p}(x(1-p))^N\right)=1-(x(1-p))^N.$$

3. On note P_1 et P_2 les polynômes définis par :

$$P_1(z)=1-p-z+pz^N,\ P_2(z)=1-z^N.$$

Le polynôme P_2 a toutes ses racines simples (ce sont les racines n-èmes de l'unité) et $z_0=1$ est la seule réelle. En écrivant que $P_1(z)=1-z-pP_2(z)$, on déduit que z_0 est l'unique racine commune à P_1 et P_2. On a alors les factorisations :

$$P_2(z)=(1-z)\sum_{k=0}^{N-1}z^k$$

et :

$$P_1(z)=(1-z)\left(1-p\sum_{k=0}^{N-1}z^k\right)$$

On en déduit que la seule racine commune à

$$Q_1(x)=1-x+\frac{p}{1-p}(x(1-p))^N=\frac{1}{1-p}P_1((1-p)x)$$

et

$$Q_2(x)=1-(x(1-p))^N=P_2((1-p)x)$$

est $x_0=\dfrac{1}{1-p}$ et cette racine est simple. On a alors les factorisations :

$$Q_1(x)=\frac{1}{1-p}(1-(1-p)x)\left(1-p\sum_{k=0}^{N-1}(1-p)^kx^k\right)$$

et :

$$Q_2(x)=(1-(1-p)x)\sum_{k=0}^{N-1}(1-p)^kx^k$$

qui donnent :

$$Q(x)=\frac{Q_2(x)}{Q_1(x)}$$

pour $x \in [-1,1] \setminus \left\{ \frac{1}{1-p} \right\}$ et après simplification :

$$Q(x) = (1-p) \frac{\sum_{k=0}^{N-1} (1-p)^k x^k}{1 - p \sum_{k=0}^{N-1} (1-p)^k x^k}.$$

pour tout $x \in [-1,1]$. En notant $B(x) = p \sum_{k=1}^{N-1} (1-p)^{k-1} x^k - 1$, on a :

$$\begin{aligned} Q(x) &= (1-p) \frac{1 + \frac{1-p}{p} (B(x)+1)}{1 - p - (1-p)(B(x)+1)} \\ &= -\frac{\frac{1-p}{p} B(x) + \frac{1}{p}}{B(x)} = -\frac{1-p}{p} - \frac{1}{pB(x)} \\ &= 1 - \frac{1}{p} - \frac{1}{pB(x)}. \end{aligned}$$

5.3. Étude des racines de B

1. La fonction polynomiale B est $\mathcal{C}^\infty$ sur $\mathbb{R}$ avec $B'(x) > 0$ pour tout $x > 0$ puisque les $(1-p)^{k-1}$ sont tous strictement positifs. La fonction B est donc continue strictement croissante sur $\mathbb{R}^+$ avec $B(0) = -1$ et $\lim_{x \to +\infty} B(x) = +\infty$ et en conséquence réalise une bijection de $\mathbb{R}^+$ sur $[-1, +\infty[$. En particulier, il existe un unique réel strictement positif ρ_N tel que $B(\rho_N) = 0$. Avec $B(1) = -(1-p)^{N-1} < 0$, on déduit que $\rho_N > 1$ (théorème des valeurs intermédiaires). Cette racine ρ_N est bien simple puisque $B'(\rho_N) > 0$.
2. Dire que $z \in \mathbb{C}$ est racine de B équivaut à dire que :

$$\sum_{k=1}^{N-1} (1-p)^{k-1} z^k = \frac{1}{p}$$

et on a :

$$\frac{1}{p} \leq \sum_{k=1}^{N-1} (1-p)^{k-1} |z|^k$$

de sorte que $|z| < \rho_N$ entraîne :

$$\frac{1}{p} < \sum_{k=1}^{N-1} (1-p)^{k-1} \rho_N^k = \frac{1}{p}$$

(ρ_N est racine de B) ce qui est impossible. On a donc $|z| \geq \rho_N$ pour toute racine complexe de B.
Supposons maintenant que z soit une racine complexe de B telle que $|z| = \rho_N$. On a alors $z \neq 0$ et :

$$\left|\sum_{k=1}^{N-1} (1-p)^{k-1} z^k\right| = \frac{1}{p} = \sum_{k=1}^{N-1} (1-p)^{k-1} \rho_N^k = \sum_{k=1}^{N-1} (1-p)^{k-1} |z|^k$$

et le lemme **5.1**. nous dit qu'il existe des réels $\lambda_k > 0$ tels que, pour tout k compris entre 2 et $N-1$, on ait $(1-p)^{k-1} z^k = \lambda_k z$. En particulier, pour $k = 2$, on a $(1-p) z^2 = \lambda_1 z$ et $z = \dfrac{\lambda_1}{1-p} \in \mathbb{R}^{+,*}$ ce qui équivaut à $z = \rho_N$ puisque ρ_N est l'unique racine positive de B.
On a donc $|z| > \rho_N$ pour toute racine complexe de B différente de ρ_N.
Au passage, on a montré que ρ_N est en fait l'unique racine réelle de B.

3. La fonction $Q(z) = 1 - \dfrac{1}{p} - \dfrac{1}{pB(z)}$ étant la somme d'une série entière normalement convergente sur le disque unité fermé, ne peut avoir de pôles dans ce disque.

5.4. Recherche d'équivalents

On note $z_1 = \rho_N, z_2, \cdots, z_m$ les racines complexes de B avec les multiplicités respectives $\nu_1 = 1, \nu_2 \geq 1, \cdots, \nu_m \geq 1$. On rappelle que, pour k compris entre 2 et m, la racine z_k est complexe non réelle et on a $1 < \rho_N = |z_1| < |z_k|$.

1. Dans $\mathbb{C}(X)$, on a la décomposition en éléments simples :

$$\frac{1}{B(X)} = \sum_{k=1}^{m} \sum_{s=1}^{\nu_k} \frac{\lambda_{k,s}}{(X - z_k)^s}$$

où les $\lambda_{k,s}$ sont des nombres complexes. Comme les racines de B sont en dehors du disque unité, l'identité précédente est valable pour tout z dans ce disque.
Pour $k = 1$, on a $\nu_1 = 1$ et :

$$\lambda_{1,1} = \frac{1}{B'(\rho_N)} > 0$$

et pour k compris entre 2 et m :

$$\lambda_{k,\nu_k} = \lim_{z \to z_k} \frac{(z - z_k)^{\nu_k}}{B(z)} \neq 0.$$

Le fait que les autres $\lambda_{k,s}$ sont différents de 0 ne me semble pas évident et de toute façon n'est pas utile pour la suite.

2.

(a) On connaît, pour tout entier $s \geq 1$, le développement en série entière :

$$\frac{1}{(1-t)^s} = \sum_{n=0}^{+\infty} C_{n+s-1}^{s-1} t^n$$

valable pour $|t| < 1$ dans $\mathbb{C}$.
On en déduit que pour tout nombre complexe z tel que $|z| \leq 1 < |z_k|$ où k est compris entre 1 et m, on a :

$$\frac{1}{(z_k - z)^s} = \frac{1}{z_k^s} \frac{1}{\left(1 - \dfrac{z}{z_k}\right)^s} = \sum_{n=0}^{+\infty} C_{n+s-1}^{s-1} \frac{z^n}{z_k^{n+s}}$$

(b) Pour tout k compris entre 1 et m, on a :

$$\begin{aligned}\sum_{s=1}^{\nu_k} \frac{\lambda_{k,s}}{(z-z_k)^s} &= \sum_{s=1}^{\nu_k} \lambda_{k,s} (-1)^k \sum_{n=0}^{+\infty} C_{n+s-1}^{s-1} \frac{z^n}{z_k^{n+s}} \\ &= \sum_{n=0}^{+\infty} \left(\sum_{s=1}^{\nu_k} (-1)^k \lambda_{k,s} C_{n+s-1}^{s-1} \frac{1}{z_k^s} \right) \frac{z^n}{z_k^n} \\ &= \sum_{n=0}^{+\infty} \left(P_k(n) \frac{1}{z_k^n} \right) z^n\end{aligned}$$

où on a posé :

$$P_k(n) = (-1)^k \sum_{s=1}^{\nu_k} \lambda_{k,s} C_{n+s-1}^{s-1} \frac{1}{z_k^s}.$$

Pour $k = 1$, on a $\nu_1 = 1$ et :

$$P_1(n) = -\lambda_{1,1} \frac{1}{z_1} = -\frac{1}{B'(\rho_N)} \frac{1}{\rho_N}$$

c'est-à-dire que P_1 est un polynôme constant non nul.
Pour k compris entre 2 et m, en écrivant que :

$$C_{n+s-1}^{s-1} = \frac{(n+s-1)!}{(s-1)!n!} = \frac{(n+s-1)\cdots(n+1)}{(s-1)!},$$

on voit que C_{n+s-1}^{s-1} est un polynôme en n de degré $s-1$ et P_k est un polynôme en n de degré au plus égal à $\nu_k - 1$.

(c) On a, pour tout $x \in \left]-1,1\right[$:

$$\begin{aligned} Q(x) = \sum_{n=0}^{+\infty} a_{n+1} x^n &= 1 - \frac{1}{p} - \frac{1}{pB(x)} \\ &= 1 - \frac{1}{p} - \frac{1}{p} \sum_{k=1}^{m} \sum_{s=1}^{\nu_k} \frac{\lambda_{k,s}}{(x - z_k)^s} \\ &= 1 - \frac{1}{p} - \frac{1}{p} \sum_{k=1}^{m} \sum_{n=0}^{+\infty} \left(P_k(n) \frac{1}{z_k^n} \right) x^n \\ &= 1 - \frac{1}{p} - \frac{1}{p} \sum_{n=0}^{+\infty} \sum_{k=1}^{m} \left(P_k(n) \frac{1}{z_k^n} \right) x^n \end{aligned}$$

et avec l'unicité du développement en série entière sur $\left]-1,1\right[$, on déduit que :

$$a_1 = 1 - \frac{1}{p} - \frac{1}{p} \sum_{k=1}^{m} P_k(0)$$

et pour $n \geq 1$:

$$a_{n+1} = -\frac{1}{p} \sum_{k=1}^{m} \frac{P_k(n)}{z_k^n}.$$

On peut remarquer que $a_1 = 1$ nous donne :

$$\sum_{k=1}^{m} P_k(0) = -1.$$

3.

(a) De :

$$a_{n+1} = -\frac{1}{p} \left(\frac{P_1(n)}{z_1^n} + \frac{P_2(n)}{z_2^n} + \cdots + \frac{P_m(n)}{z_m^n} \right)$$

avec $P_1(n) < 0$ et $\rho_N = |z_1| < |z_k|$ pour $k \geq 2$, on déduit que :

$$a_{n+1} \underset{+\infty}{\backsim} -\frac{1}{p} \frac{P_1(n)}{z_1^n} = \frac{1}{p} \frac{1}{B'(\rho_N)} \frac{1}{\rho_N^{n+1}} = \frac{K}{\rho_N^{n+1}}$$

avec $K = \dfrac{1}{p} \dfrac{1}{B'(\rho_N)} > 0$.

(b) De $\mathbb{P}(T = n) = g_{n-N+1} = a_{n-N+1} p (1-p)^{N-1}$, on déduit que :

$$\mathbb{P}(T = n) \underset{+\infty}{\backsim} p (1-p)^{N-1} \frac{K}{\rho_N^{n-N+1}} = \frac{(1-p)^{N-1}}{B'(\rho_N)} \rho_N^N \frac{1}{\rho_N^{n+1}}.$$

Chapitre 2

CAPES externe 2007, épreuve 1

2.1 Énoncé

INTRODUCTION

L'objet du problème est l'étude de la suite $(s_n)_{n\geq 1}$ définie par :

$$\forall n \geq 1,\ s_n = \sum_{k=1}^{n} \frac{1}{k^2}$$

Dans une première partie, nous nous attacherons à démontrer, de plusieurs façons, par des méthodes élémentaires, que cette suite converge. Les parties **2**, **3** et **4** suivantes seront consacrées à la détermination de sa limite S par divers moyens. Les parties **5** et **6** utiliseront la valeur de S pour calculer la somme de certaines séries numériques.

– I – Convergence de la suite

Dans cette partie, le candidat utilisera librement les connaissances faisant partie du programme de Terminale S.

1. *Première méthode*

   (a) Démontrer que, pour tout entier $k \geq 2$, on a la majoration

   $$\frac{1}{k^2} \leq \frac{1}{k-1} - \frac{1}{k}.$$

(b) En déduire que la suite $(s_n)_{n\geq 1}$ est majorée.

(c) Démontrer que la suite $(s_n)_{n\geq 1}$ converge et donner un majorant de sa limite.

Dans toute la suite du problème, on notera S cette limite.

2. *Deuxième méthode*
On considère la suite $(t_n)_{n\geq 1}$, définie par :

$$\forall n \geq 1,\ t_n = s_n + \frac{1}{n}.$$

(a) Démontrer que les suites $(s_n)_{n\geq 1}$ et $(t_n)_{n\geq 1}$ sont adjacentes.

(b) Donner, en le justifiant, un encadrement d'amplitude 10^{-1} de S.

3. *Troisième méthode*
Ecrire le texte d'un exercice de niveau terminale S démontrant, par comparaison à une intégrale, la convergence de la suite $(s_n)_{n\geq 1}$.

– II – Utilisation de polynômes

1. Soit $P \in \mathbb{C}[X]$ un polynôme de degré $n \geq 1$: $P(X) = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$.
Rappeler la formule permettant de calculer la somme $\sigma_1 = \sum\limits_{i=1}^{n} \alpha_i = \alpha_1 + \cdots + \alpha_n$ des racines de P en fonction de ces coefficients a_k, $k \in \{0, \cdots, n\}$.

2.

(a) Soient $p \in \mathbb{N}$ et $\varphi \in \mathbb{R}$. Démontrer l'égalité :

$$\sin((2p+1)\varphi) = \sum_{k=0}^{p} (-1)^k \begin{pmatrix} 2p+1 \\ 2k+1 \end{pmatrix} \cos^{2p-2k}(\varphi) \sin^{2k+1}(\varphi).$$

où $\begin{pmatrix} 2p+1 \\ 2k+1 \end{pmatrix}$ désigne le coefficient binomial pour $k \in \{0, \cdots, p\}$.

(b) En déduire que, pour tout entier $p \in \mathbb{N}$ et tout réel $\varphi \not\equiv 0\,[\pi]$, on a :

$$\sin((2p+1)\varphi) = \sin^{2p+1}(\varphi) \sum_{k=0}^{p} (-1)^k \begin{pmatrix} 2p+1 \\ 2k+1 \end{pmatrix} \left(\mathrm{cotan}^2(\varphi)\right)^{p-k}$$

où $\mathrm{cotan}(\varphi) = \dfrac{\cos(\varphi)}{\sin(\varphi)}$.

3. Soit $p \in \mathbb{N}$ et $P \in \mathbb{R}[X]$ le polynôme défini par :

$$P(X) = \sum_{k=0}^{p} (-1)^k \binom{2p+1}{2k+1} X^{p-k}.$$

   (a) Pour tout entier $k \in \{1, \cdots, p\}$, on pose $\gamma_k = \operatorname{cotan}^2\left(\frac{k\pi}{2p+1}\right)$. Calculer $P(\gamma_k)$ pour tout $k \in \{1, \cdots, p\}$.

   (b) Vérifier que, pour tout $k \in \{1, \cdots, p\}$, le réel $\frac{k\pi}{2p+1}$ appartient à l'intervalle $\left]0, \frac{\pi}{2}\right[$. En déduire que le polynôme P possède p racines distinctes, que l'on déterminera.

   (c) En déduire les égalités :

$$\sum_{k=1}^{p} \operatorname{cotan}^2\left(\frac{k\pi}{2p+1}\right) = \frac{p(2p-1)}{3}$$

$$\sum_{k=1}^{p} \frac{1}{\sin^2\left(\frac{k\pi}{2p+1}\right)} = \frac{2p(p+1)}{3}.$$

4.

   (a) Démontrer, pour tout réel $\varphi \in]0, \frac{\pi}{2}[$, les encadrements :

$$0 < \sin\varphi < \varphi < \tan\varphi$$

   (b) En déduire que, pour tout entier $p \geq 1$, on a l'encadrement :

$$\frac{p(2p-1)}{3} < \frac{(2p+1)^2}{\pi^2} \sum_{k=1}^{p} \frac{1}{k^2} < \frac{2p(p+1)}{3}.$$

   (c) Démontrer que $S = \frac{\pi^2}{6}$.

5. Montrer que les suites $(u_n)_{n\geq 1}$, $(v_n)_{n\geq 1}$ et $(w_n)_{n\geq 1}$ définies par :

$$\forall n \geq 1,\ u_n = \sum_{k=1}^{n} \frac{1}{(2k)^2},\ v_n = \sum_{k=0}^{n} \frac{1}{(2k+1)^2},\ w_n = \sum_{k=1}^{n} \frac{(-1)^{k+1}}{k^2}$$

sont convergentes et déterminer les valeurs exactes de leurs limites, respectivement notées U, V et W.

– III – Utilisation des intégrales de Wallis

Pour tout entier $n \in \mathbb{N}$, on pose :

$$I_n = \int_0^{\frac{\pi}{2}} \cos^{2n}(t)\,dt, \quad J_n = \int_0^{\frac{\pi}{2}} t^2 \cos^{2n}(t)\,dt \text{ et } K_n = \frac{4^n\,(n!)^2}{(2n))} J_n.$$

1. Calculer les intégrales I_0 et J_0.
2.
   (a) Démontrer que pour tout $n \in \mathbb{N}$, on a : $I_{n+1} = \dfrac{2n+1}{2n+2} I_n$.
   (*Indication : on pourra penser à l'intégration par parties.*)

   (b) En déduire que pour tout $n \in \mathbb{N}$, on a : $I_n = \dfrac{(2n)!}{4^n (n!)^2} \dfrac{\pi}{2}$.
3. Soit $n \geq 1$.

   (a) Démontrer la relation :

   $$I_n = n\,(2n-1)\,J_{n-1} - 2n^2 J_n.$$

   (b) En déduire que :

   $$K_{n-1} - K_n = \frac{\pi}{4n^2}.$$

   (c) Démontrer la relation :

   $$\frac{\pi}{4} \sum_{k=1}^{n} \frac{1}{k^2} = J_0 - K_n.$$
4.
   (a) Démontrer que, pour tout réel $x \in [0, \frac{\pi}{2}]$, on a : $x \leq \frac{\pi}{2} \sin x$.

   (b) En déduire que, pour tout entier n, on a :

   $$0 \leq J_n \leq \frac{\pi^2 I_n}{8\,(n+1)}, \text{ puis } 0 \leq K_n \leq \frac{\pi^3}{16\,(n+1)}$$

   (c) Retrouver la valeur de S.

– IV – Noyau de Dirichlet

Pour tout entier $n \geq 1$, on note D_n le *noyau de* Dirichlet, défini par :

$$\forall x \in \mathbb{R},\ D_n(x) = \frac{1}{2} + \sum_{k=1}^{n} \cos(kx).$$

1. Démontrer que, pour tout entier $n \geq 1$ et tout réel $x \not\equiv 0\,[2\pi]$, on a :

$$D_n(x) = \frac{1}{2}\frac{\sin\left(n+\frac{1}{2}\right)x}{\sin\left(\frac{x}{2}\right)}$$

2. Pour tout entier $n \geq 1$, on note L_n l'intégrale :

$$L_n = \int_0^{\pi} x D_n(x)\,dx$$

   (a) Calculer l'intégrale $\displaystyle\int_0^{\pi} x\cos(kx)\,dx$ pour tout entier $k \geq 1$.

   (b) En déduire que :

$$L_n = \frac{\pi^2}{4} - \sum_{k=1}^{n}\frac{1}{k^2} + \sum_{k=1}^{n}(-1)^k\frac{1}{k^2}.$$

3. On note f le prolongement par continuité en 0 de la fonction définie sur l'intervalle $]0,\pi]$ par :

$$x \mapsto \frac{x}{\sin\left(\frac{x}{2}\right)}.$$

   Démontrer que la fonction f est de classe $\mathcal{C}^1$ sur l'intervalle $[0,\pi]$.

4. Soit $\phi : [0,\pi] \to \mathbb{R}$ une fonction de classe $\mathcal{C}^1$ sur $[0,\pi]$. Démontrer que :

$$\lim_{\lambda\to+\infty}\int_0^{\pi}\phi(x)\,\sin(\lambda x)\,dx = 0.$$

   (*Indication : on pourra penser à l'intégration par parties.*)

5.

   (a) Démontrer que $\lim_{n\to+\infty} L_n = 0$.

   (b) Retrouver la valeur de S. (On utilisera la relation entre W et S obtenue à la question **5** de la deuxième partie.)

– V – Une somme double

L'objet de cette partie est de calculer la limite de la somme double :

$$\lim_{M\to+\infty}\left(\lim_{N\to+\infty}\sum_{n=1}^{N}\sum_{m=1}^{M}\frac{1}{nm\,(n+m-1)}\right).$$

On pose pour tout entier $N \geq 1$, $H_N = \sum\limits_{n=1}^{N}\frac{1}{n}$.

1.

   (a) Démontrer que pour tout entier $N \geq 1$, on a :

   $$\ln(1+N) \leq H_N \leq 1+\ln(N).$$

   (b) En déduire que $\lim\limits_{N\to+\infty}\frac{H_N}{N} = 0$.

   (c) Démontrer que pour tout entier $M \geq 2$, on a :

   $$\sum_{m=1}^{M-1}\frac{H_m}{m\,(m+1)} = \sum_{m=1}^{M}\frac{1}{m^2} - \frac{H_M}{M}.$$

   (d) En déduire que la série $\sum\limits_{m=1}^{+\infty}\frac{H_m}{m\,(m+1)}$ converge et déterminer sa limite.

2. Pour tout entier $N \geq 1$ et pour tout entier $m \geq 2$, on pose :

   $$Z_{N,m} = \sum_{n=1}^{N}\frac{1}{n\,(n+m-1)}.$$

   (a) Démontrer que pour tout entier $m \geq 2$:

   $$Z_{N,m} = \frac{1}{m-1}\left(H_{m-1} - \sum_{n=N+1}^{N+m-1}\frac{1}{n}\right).$$

   (b) En déduire que $\lim\limits_{N\to+\infty} Z_{N,m} = \frac{H_{m-1}}{m-1}$.

3.

(a) Montrer que pour tout entier $N \geq 1$ et pour tout entier $M \geq 2$, on a :

$$\sum_{n=1}^{N} \sum_{m=1}^{M} \frac{1}{nm\,(n+m-1)} = \sum_{n=1}^{N} \frac{1}{n^2} + \sum_{m=2}^{M} \frac{Z_{N,m}}{m}.$$

(b) Montrer que :

$$\lim_{N \to +\infty} \sum_{n=1}^{N} \sum_{m=1}^{M} \frac{1}{nm\,(n+m-1)} = \frac{\pi^2}{6} + \sum_{m=2}^{M} \frac{H_{m-1}}{m\,(m-1)}.$$

(c) En déduire alors :

$$\lim_{M \to +\infty} \left(\lim_{N \to +\infty} \sum_{n=1}^{N} \sum_{m=1}^{M} \frac{1}{nm\,(n+m-1)} \right).$$

– VI – La fonction Dilogarithme

Pour tout réel $x \in [-1, 1[$, on considère l'intégrale :

$$L_i(x) = -\int_0^x \frac{\ln(1-t)}{t} t.$$

1. Justifier l'existence de cette intégrale pour tout réel $x \in [-1, 1[$.
2. On définit la fonction Dilogarithme

$$L_i : \begin{array}{ccc} [-1, 1[& \to & \mathbb{R} \\ x & \mapsto & L_i\,(x) \end{array}$$

   Démontrer que la fonction L_i est prolongeable par continuité en 1. On notera encore L_i ce prolongement par continuité.
3.

   (a) Démontrer que pour tout $x \in]-1, 1[$, on a :

$$L_i\,(x) = \sum_{n=1}^{+\infty} \frac{x^n}{n^2}.$$

   (b) En déduire la valeur de $L_i\,(1)$.

(c) Démontrer la relation fonctionnelle :

$$\forall x \in \left]0,1\right[,\ L_i(x) + L_i(1-x) = \frac{\pi^2}{6} - \ln(1-x)\ln(x).$$

4. Déduire de la question précédente, la valeur de la somme $\sum\limits_{n=1}^{+\infty} \frac{1}{2^n n^2}$.

5.

(a) Pour tout réel $x \in \left]-1,1\right[$, démontrer la relation :

$$L_i(x) + L_i(-x) = \frac{1}{2} L_i\left(x^2\right).$$

(b) Retrouver la valeur de la somme $\sum\limits_{n=1}^{+\infty} \frac{(-1)^n}{n^2}$.

6.

(a) Pour tout réel $x \in \left]0,1\right[$, démontrer la relation :

$$L_i(x) - L_i(-x) + L_i\left(\frac{1-x}{1+x}\right) - L_i\left(\frac{x-1}{1+x}\right) = \frac{\pi^2}{4} + \ln\left(\frac{1+x}{1-x}\right)\ln(x)$$

(b) En déduire la valeur de la somme $\sum\limits_{n=0}^{+\infty} \frac{(\sqrt{2}-1)^{2n+1}}{(2n+1)^2}$.

2.2 Corrigé

– I – Convergence d'une suite

1.

(a) Pour $k \geq 2$, on a :

$$\frac{1}{k^2} < \frac{1}{k(k-1)} = \frac{1}{k-1} - \frac{1}{k}.$$

De manière plus générale, on a pour tout réel $\alpha > 0$ et tout entier $k \geq 2$:

$$\frac{1}{k^\alpha} < \frac{1}{\alpha - 1}\left(\frac{1}{(k-1)^{\alpha-1}} - \frac{1}{k^{\alpha-1}}\right).$$

En effet, on a :

$$\frac{1}{k^\alpha} < \int_{k-1}^{k} \frac{dt}{t^\alpha} = \left[-\frac{1}{\alpha-1}\frac{1}{t^{\alpha-1}}\right]_{k-1}^{k}$$
$$= \frac{1}{\alpha-1}\left(\frac{1}{(k-1)^{\alpha-1}} - \frac{1}{k^{\alpha-1}}\right)$$

(b) Pour $n \geq 2$, on a :

$$\begin{aligned} s_n = 1 + \sum_{k=2}^{n} \frac{1}{k^2} &\leq 1 + \sum_{k=2}^{n} \left(\frac{1}{k-1} - \frac{1}{k} \right) \\ &\leq 1 + \sum_{k=2}^{n} \frac{1}{k-1} - \sum_{k=2}^{n} \frac{1}{k} \\ &\leq 1 + \sum_{k=1}^{n-1} \frac{1}{k} - \sum_{k=2}^{n} \frac{1}{k} = 2 - \frac{1}{n} \leq 2. \end{aligned}$$

De manière plus générale, pour $\alpha > 1$ et $n \geq 2$, on a :

$$\begin{aligned} s_n = 1 + \sum_{k=2}^{n} \frac{1}{k^\alpha} &\leq 1 + \frac{1}{\alpha - 1} \sum_{k=2}^{n} \left(\frac{1}{(k-1)^{\alpha-1}} - \frac{1}{k^{\alpha-1}} \right) \\ &\leq 1 + \frac{1}{\alpha - 1} \left(\sum_{k=2}^{n} \frac{1}{(k-1)^{\alpha-1}} - \sum_{k=2}^{n} \frac{1}{k^{\alpha-1}} \right) \\ &\leq 1 + \frac{1}{\alpha - 1} \left(\sum_{k=1}^{n-1} \frac{1}{k^{\alpha-1}} - \sum_{k=2}^{n} \frac{1}{k^{\alpha-1}} \right) \\ &\leq 1 + \frac{1}{\alpha - 1} - \frac{1}{\alpha - 1} \frac{1}{n^{\alpha-1}} \leq 1 + \frac{1}{\alpha - 1}. \end{aligned}$$

(c) La suite $(s_n)_{n \geq 1}$ étant croissante (sommes de réels positifs) et majorée est convergente de limite $S \in]0, 2]$ (resp. $S \in \left]0, 1 + \frac{1}{\alpha - 1}\right]$ pour $\alpha > 1$).

2. On va montrer de manière un plus générale, en utilisant le théorème sur les suites adjacentes, que, pour tout réel $\alpha \geq 2$, la série $\sum \frac{1}{n^\alpha}$ est convergente. Pour ce faire on utilise les suites $(s_n)_{n \geq 1}$ et $(t_n)_{n \geq 1}$ définies par :

$$s_n = \sum_{k=1}^{n} \frac{1}{k^\alpha} \text{ et } t_n = s_n + \frac{1}{n^{\alpha-1}}.$$

(a) La suite $(s_n)_{n \geq 1}$ est croissante puisque chaque terme s_n est somme de réels positifs.
Pour tout $n \geq 1$, on a :

$$t_{n+1} - t_n = \frac{1}{(n+1)^\alpha} - \left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}} \right)$$

avec :

$$\frac{1}{(n+1)^{\alpha}} < \frac{1}{\alpha-1}\left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}\right)$$

ce qui donne :

$$t_{n+1} - t_n < \left(\frac{1}{\alpha-1} - 1\right)\left(\frac{1}{n^{\alpha-1}} - \frac{1}{(n+1)^{\alpha-1}}\right) \leq 0$$

pour $\alpha \geq 2$ (dans ce cas $\frac{1}{\alpha-1} - 1 = \frac{2-\alpha}{\alpha-1} \leq 0$), ce qui signifie que la suite $(t_n)_{n\geq 1}$ est décroissante
Enfin avec :

$$\lim_{n\to+\infty}(t_n - s_n) = \lim_{n\to+\infty}\frac{1}{n^{\alpha-1}} = 0,$$

on conclut que ces deux suites sont adjacentes et donc convergentes vers une même limite S.

(b) En choisissant n tel que $\frac{1}{n^{\alpha-1}} \leq \varepsilon$, les encadrements $u_n \leq S \leq t_n$, nous permettent de donner des valeurs approchées de S d'amplitude ε. Par exemple, pour $\alpha = 2$ et $n = 10$, on obtient :

$$s_{10} = \frac{1968\,329}{1270\,080} \approx 1.549 \leq S \leq t_{10} = \frac{2095\,337}{1270\,080} \approx 1.649.$$

3. L'utilisation des primitives de $\frac{1}{x^2}$ et de sommes télescopiques pour obtenir la convergence de la série $\sum \frac{1}{n^2}$ peut être expliqué en terminale avec l'exercice élémentaire suivant.
Soient $F : [1,+\infty[\to \mathbb{R}$ une fonction majorée, dérivable de dérivée $F' = f$ positive et décroissante sur $[1,+\infty[$ (par exemple $F(x) = -\frac{1}{x} < 0$ et $f(x) = \frac{1}{x^2} > 0$) et $(s_n)_{n\geq 1}$ la suite définie par :

$$\forall n \geq 1,\ s_n = \sum_{k=1}^{n} f(k).$$

(a) Montrer que la suite $(s_n)_{n\geq 1}$ est croissante. Chaque terme s_n est somme de réels positifs.

(b) Montrer que :

$$\forall k \geq 2,\ f(k) \leq F(k) - F(k-1)$$

Comme f est décroissante, on a :

$$f(k) \leq \int_{k-1}^{k} f(t)\,dt = F(k) - F(k-1)$$

(c) Montrer que $(s_n)_{n\geq 1}$ est majorée. Pour $n \geq 2$, on a :

$$\begin{aligned} s_n = f(1) + \sum_{k=2}^{n} f(k) &\leq f(1) + \sum_{k=2}^{n} (F(k) - F(k-1)) \\ &\leq f(1) + \sum_{k=2}^{n} F(k) - \sum_{k=2}^{n} F(k-1) \\ &\leq f(1) + \sum_{k=2}^{n} F(k) - \sum_{k=1}^{n-1} F(k) \\ \leq f(1) + F(n) - F(1) &\leq f(1) + M - F(1) = L \end{aligned}$$

où M est un majorant de F.

(d) Conclure. Il en résulte que $(s_n)_{n\geq 1}$ est convergente de limite $S \in]0, L]$.

– II – Utilisation de polynômes

1. Comme $\mathbb{C}$ est algébriquement clos (théorème de d'Alembert-Gauss), tout polynôme $P(X) = \sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$ de degré $n \geq 1$ (donc $_n \neq 0$) peut être factorisé sous la forme :

$$P(X) = a_n \prod_{k=1}^{n} (X - \lambda_k).$$

En développant l'expression de droite, on en déduit par identification des coefficients des X^k, pour k compris entre 1 et n, les relations entre racines et coefficients :

$$a_{n-k} = a_n (-1)^k \sum_{1\leq i_1 < \cdots < i_k \leq n} \lambda_{i_1} \lambda_{i_2} \cdots \lambda_{i_k}$$

et en particulier :

$$a_{n-1} = -a_n \sum_{i=1}^{n} \lambda_i = -a_n \sigma_1.$$

2.

(a) Les formules suivantes, valables pour $\varphi \in \mathbb{R}$ et $n \in \mathbb{Z}$:

$$\begin{cases} \cos(\varphi) = \Re\left(e^{i\varphi}\right) \\ \sin(\varphi) = \Im\left(e^{i\varphi}\right) \end{cases}$$

(formules d'Euler) et :

$$(\cos(\varphi) + i\sin(\varphi))^n = \left(e^{i\varphi}\right)^n = e^{in\varphi} = \cos(n\varphi) + i\sin(n\varphi)$$

(formule de Moivre) permettent d'obtenir relativement facilement des formules de trigonométrie.
En utilisant la formule du binôme de Newton pour $n \in \mathbb{N}$, la formule de Moivre s'écrit :

$$\cos(n\varphi) + i\sin(n\varphi) = \sum_{k=0}^{n} C_n^k \cos^{n-k}(\varphi)\sin^k(\varphi)\, i^k$$

et l'identification des parties réelles et imaginaires permet d'exprimer $\cos(n\varphi)$ et $\sin(n\varphi)$ comme combinaisons linéaires de puissances de $\cos(\varphi)$ et $\sin(\varphi)$.
Pour $n = 2p+1$, on obtient :

$$\begin{aligned} \cos((2p+1)\varphi) + i\sin((2p+1)\varphi) &= \sum_{k=0}^{2p+1} C_{2p+1}^k \cos^{2p+1-k}(\varphi)\sin^k(\varphi)\, i^k \\ &= \sum_{k=0}^{p} C_{2p+1}^{2k} \cos^{2(p-k)+1}(\varphi)\sin^{2k}(\varphi)(-1)^k \\ &\quad + \sum_{k=0}^{p} C_{2p+1}^{2k+1} \cos^{2(p-k)}(\varphi)\sin^{2k+1}(\varphi)(-1)^k\, i \end{aligned}$$

et, pour k compris entre 0 et n :

$$\cos((2p+1)\varphi) = \sum_{k=0}^{p} (-1)^k C_{2p+1}^{2k} \cos^{2(p-k)+1}(\varphi)\sin^{2k}(\varphi)$$

$$\sin((2p+1)\varphi) = \sum_{k=0}^{p} (-1)^k C_{2p+1}^{2k+1} \cos^{2(p-k)}(\varphi)\sin^{2k+1}(\varphi)$$

(b) Pour $\sin(\varphi) \neq 0$, on peut écrire :

$$\begin{aligned}\sin((2p+1)\varphi) &= \sin^{2p+1}(\varphi)\sum_{k=0}^{p}(-1)^k C_{2p+1}^{2k+1}\frac{\cos^{2(p-k)}(\varphi)}{\sin^{2(p-k)}(\varphi)} \\ &= \sin^{2p+1}(\varphi)\sum_{k=0}^{p}(-1)^k C_{2p+1}^{2k+1}\operatorname{cotan}^{2(p-k)}(\varphi)\end{aligned}$$

3.

(a) Notant $\varphi_k = \dfrac{k\pi}{2p+1}$ et $\gamma_k = \operatorname{cotan}^2(\varphi_k)$ pour k compris entre 1 et p, on a :

$$\begin{aligned}0 = \sin((2p+1)\varphi_k) &= \sin^{2p+1}(\varphi_k)\sum_{j=0}^{p}(-1)^j C_{2p+1}^{2j+1}\gamma_k^{p-j} \\ &= \sin^{2p+1}(\varphi_k)P(\gamma_k)\end{aligned}$$

et $P(\gamma_k) = 0$.

(b) Pour $1 \leq k \leq p$, on a

$$0 < \frac{\pi}{2p+1} \leq \varphi_k = \frac{p\pi}{2p+1} < \frac{\pi}{2}$$

et la suite $(\gamma_k)_{1\leq k\leq p}$ est strictement décroissante dans $\mathbb{R}^{+,*}$ (la fonction tan est strictement croissante de $\left]0, \dfrac{\pi}{2}\right[$ sur $\mathbb{R}^{+,*}$). Comme ces γ_k fournissent p racines distinctes du polynôme P qui est de degré p, on a ainsi toutes les racines réelles de P.

(c) La somme des racines de P est :

$$\sum_{k=1}^{p}\gamma_k = \sum_{k=1}^{p}\operatorname{cotan}^2(\varphi_k) = -\frac{a_{p-1}}{a_p} = \frac{C_{2p+1}^3}{C_{2p+1}^1} = \frac{p(2p-1)}{3}$$

ce qui peut aussi s'écrire, en tenant compte de :

$$\operatorname{cotan}^2(\varphi_k) = \frac{1}{\sin^2(\varphi_k)} - 1$$

$$\sum_{k=1}^{p}\frac{1}{\sin^2(\varphi_k)} = \frac{p(2p-1)}{3} + p = \frac{2p(p+1)}{3}$$

4.

(a) En utilisant le théorème des accroissements finis, on a, pour tout réel $\varphi \in \left]0, \frac{\pi}{2}\right[$:

$$\begin{cases} 0 < \sin(\varphi) = \sin(\varphi) - \sin(0) = \varphi \cos(c_\varphi) < \varphi \\ \tan(\varphi) = \tan(\varphi) - \tan(0) = \varphi\left(1 + \tan^2(d_\varphi)\right) > \varphi > 0 \end{cases}$$

avec $0 < c_\varphi, d_\varphi < \varphi$, ce qui donne :

$$0 < \sin(\varphi) < \varphi < \tan(\varphi)$$

ou encore :

$$0 < \operatorname{cotan}(\varphi) = \frac{1}{\tan(\varphi)} < \frac{1}{\varphi} < \frac{1}{\sin(\varphi)}.$$

(b) En utilisant l'encadrement précédent, on a pour tout k compris entre 1 et p :

$$\operatorname{cotan}^2(\varphi_k) < \frac{(2p+1)^2}{k^2\pi^2} < \frac{1}{\sin^2(\varphi_k)}$$

et en sommant :

$$\sum_{k=1}^{p} \operatorname{cotan}^2(\varphi_k) < \frac{(2p+1)^2}{\pi^2} \sum_{k=1}^{n} \frac{1}{k^2} < \sum_{k=1}^{p} \frac{1}{\sin^2(\varphi_k)}$$

soit :

$$\frac{p(2p-1)}{3} < \frac{(2p+1)^2}{\pi^2} \sum_{k=1}^{n} \frac{1}{k^2} < \frac{2p(p+1)}{3}.$$

(c) En écrivant l'inégalité précédente sous la forme :

$$\frac{\pi^2}{6} < \frac{(2p+1)^2}{2p(2p-1)} \sum_{k=1}^{n} \frac{1}{k^2} < \frac{2p(p+1)}{p(2p-1)} \frac{\pi^2}{6}$$

et faisant tendre p vers l'infini, on déduit que $S = \sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

5. En écrivant que :

$$S = \sum_{n=1}^{+\infty} \frac{1}{n^2} = \sum_{n=1}^{+\infty} \frac{1}{(2n)^2} + \sum_{n=1}^{+\infty} \frac{1}{(2n+1)^2} = \frac{S}{4} + \sum_{n=1}^{+\infty} \frac{1}{(2n+1)^2}$$

on déduit que :

$$\sum_{n=1}^{+\infty} \frac{1}{(2n+1)^2} = \frac{3}{4}S = \frac{\pi^2}{8}$$

Avec $\left|\frac{(-1)^{n+1}}{n^2}\right| = \frac{1}{n^2}$, on déduit que la série $\sum \frac{(-1)^n}{n^2}$ est absolument convergente et on a :

$$\begin{aligned}\sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n^2} &= -\sum_{n=1}^{+\infty} \frac{1}{(2n)^2} + \sum_{n=1}^{+\infty} \frac{1}{(2n+1)^2} = -\frac{S}{4} + \frac{3}{4}S \\ &= \frac{1}{2}S = \frac{\pi^2}{12}.\end{aligned}$$

Remarques

On peut aussi procéder de la façon suivante.
Tout d'abord l'introduction du polynôme P est motivée par le résultat suivant : pour tout entier naturel n, les racines complexes de l'équation :

$$(z+1)^{2n+1} = (z-1)^{2n+1} \tag{2.1}$$

sont données par :

$$z_k = i \operatorname{cotan}\left(\frac{k\pi}{2n+1}\right) \quad (k \neq 0 \text{ et } -n \leq k \leq n)$$

Si $z \in \mathbb{C}$ est solution de (2.1), on a alors $z \neq 1$ et $Z = \frac{z+1}{z-1}$ est solution de $Z^{2n+1} = 1$, c'est donc une racine $(2n+1)$-ème de l'unité, c'est-à-dire qu'il existe un entier p compris entre 0 et $2n$ tel que :

$$Z = e^{i\frac{2p\pi}{2n+1}}.$$

En écrivant tout entier p compris entre $n+1$ et $2n$, sous la forme $p = 2n+1-k$ avec k compris entre 1 et n, on a :

$$e^{i\frac{2p\pi}{2n+1}} = e^{i\frac{2(2n+1-k)\pi}{2n+1}} = e^{2i\pi}e^{-i\frac{2k\pi}{2n+1}} = e^{-i\frac{2k\pi}{2n+1}}.$$

On a donc :

$$Z \in \left\{e^{i\frac{2k\pi}{2n+1}} \mid 0 \leq k \leq n\right\} \cup \left\{e^{-i\frac{2k\pi}{2n+1}} \mid 1 \leq k \leq n\right\}$$

ou encore :

$$Z \in S_n = \left\{ e^{i\frac{2k\pi}{2n+1}} \mid -n \leq k \leq n \right\}.$$

En écrivant que :

$$\left(z \neq 1 \text{ et } Z = \frac{z+1}{z-1} \right) \Leftrightarrow \left(Z \neq 1 \text{ et } z = \frac{Z+1}{Z-1} \right)$$

(la fonction homographique $z \mapsto \dfrac{z+1}{z-1}$ réalise une bijection de $\mathbb{C} \setminus \{1\}$ sur lui même), on déduit que si $z \in \mathbb{C}$ est solution de (2.1), alors $Z \in S_n \setminus \{1\}$ et il existe un entier k non nul compris entre $-n$ et n tel que :

$$\begin{aligned} z &= \frac{e^{i\frac{2k\pi}{2n+1}} + 1}{e^{i\frac{2k\pi}{2n+1}} - 1} = \frac{e^{i\frac{k\pi}{2n+1}} + e^{-i\frac{k\pi}{2n+1}}}{e^{i\frac{k\pi}{2n+1}} - e^{-i\frac{k\pi}{2n+1}}} = \frac{\cos\left(\frac{k\pi}{2n+1}\right)}{i\sin\left(\frac{k\pi}{2n+1}\right)} \\ &= -i \operatorname{cotan}\left(\frac{k\pi}{2n+1}\right) \end{aligned}$$

La fonction cotan étant impaire, cela s'écrit aussi :

$$z = z_k = i \operatorname{cotan}\left(\frac{k\pi}{2n+1}\right) \ (k \neq 0 \text{ et } -n \leq k \leq n).$$

La fonction tan qui est strictement croissante sur $\left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[$ est injective et en conséquence $z_k \neq z_j$ pour $k \neq j$ dans $\{-n, \cdots, -1, 1, \cdots, n\}$ (les z_k sont bien dans $\left]-\dfrac{\pi}{2}, \dfrac{\pi}{2}\right[$) c'est-à-dire qu'on a obtenu $2n$ racines distinctes de l'équation (2.1). Comme cette équation est exactement de degré $2n$ (en développant avec la formule du binôme cette équation s'écrit $2(2n+1)z^{2n} + \cdots = 0$), on a bien toutes les racines.

Ensuite, on vérifie que l'équation (2.1) peut s'écrire :

$$\sum_{k=0}^{n} C_{2n+1}^{2k+1} z^{2n-2k} = 0 \tag{2.2}$$

c'est-à-dire que si $z \in \mathbb{C}$ est solution de (2.1), alors $u = z^2$ est solution de :

$$P_n(u) = \sum_{k=0}^{n} C_{2n+1}^{2k+1} u^{n-k} = 0 \tag{2.3}$$

En écrivant que :

$$\begin{cases} (z+1)^{2n+1} = \sum\limits_{j=0}^{n} C_{2n+1}^{j} z^{2n+1-j} = \sum\limits_{k=0}^{n} C_{2n+1}^{2k} z^{2n+1-2k} + \sum\limits_{k=0}^{n} C_{2n+1}^{2k+1} z^{2n+1-(2k+1)} \\ (z-1)^{2n+1} = \sum\limits_{j=0}^{n} C_{2n+1}^{j} (-1)^j z^{2n+1-j} = \sum\limits_{k=0}^{n} C_{2n+1}^{2k} z^{2n+1-2k} - \sum\limits_{k=0}^{n} C_{2n+1}^{2k+1} z^{2n+1-(2k+1)} \end{cases}$$

on déduit que :

$$Q_{2n}(z) = (z+1)^{2n+1} - (z-1)^{2n+1} = 2\sum_{k=0}^{n} C_{2n+1}^{2k+1} z^{2n-2k}$$

et l'équation (2.1) est bien équivalente à l'équation (2.3) (on détaille les pointillés de la question précédente).
Comme $Q_{2n}(z) = P_n(z^2)$, on déduit que les $u_k = z_k^2 = -\operatorname{cotan}^2\left(\frac{k\pi}{2n+1}\right)$, où k est compris entre 1 et n sont des racines de P_n. Comme P_n est de degré n et les u_k, pour k compris entre 1 et n, sont deux à deux distincts (la fonction cotan est strictement décroissante sur $\left]0, \frac{\pi}{2}\right[$ et à valeurs strictement positives), on a ainsi toutes les racines de P_n. La somme des racines du polynôme P_n est :

$$\sum_{k=1}^{n} u_k = -\sum_{k=1}^{n} \operatorname{cotan}^2\left(\frac{k\pi}{2n+1}\right) = -\frac{C_{2n+1}^3}{C_{2n+1}^1} = -\frac{n(2n-1)}{3}.$$

On retrouve donc :

$$T_n = \sum_{k=1}^{n} \operatorname{cotan}^2\left(\frac{k\pi}{2n+1}\right) = \frac{n(2n-1)}{3}.$$

Pour $n=1$, on a bien $\operatorname{cotan}^2\left(\frac{\pi}{3}\right) = \frac{1}{3}$.
Il en résulte que :

$$R_n = \sum_{k=1}^{n} \frac{1}{\sin^2\left(\frac{k\pi}{2n+1}\right)} = \frac{2n(n+1)}{3}$$

On conclut alors comme dans la partie **II.**
L'idée de cette preuve est due à Ioannis Papadimitriou (the American Mathematical Monthly, Vol. 80, avril 1973, pages 424-425).

– III – Utilisation des intégrales de Wallis

1. On a $I_0 = \frac{\pi}{2}$ et $I_0 = \frac{\pi^3}{24}$.
2.

(a) Une intégration par parties donne :

$$\begin{aligned}\int_0^{\frac{\pi}{2}} \cos^{2n+1}(t)\cos(t)\,dt &= (2n+1)\int_0^{\frac{\pi}{2}} \cos^{2n}(t)\sin^2(t)\,dt \\ &= (2n+1)(I_n - I_{n+1})\end{aligned}$$

et :

$$I_{n+1} = \frac{2n+1}{2n+2} I_n.$$

(b) On procède par récurrence sur $n \geq 0$.
Pour $n = 0$, c'est vrai.
Supposant le résultat acquis au rang $n \geq 0$, on a :

$$I_{n+1} = \frac{2n+1}{2n+2}\frac{(2n)!}{4^n (n!)^2}\frac{\pi}{2} = \frac{(2n+2)!}{4^{n+1}((n+1)!)^2}\frac{\pi}{2}$$

On a donc, pour tout $n \geq 0$:

$$I_n = \frac{(2n)!}{4^n (n!)^2}\frac{\pi}{2} = \frac{J_n}{K_n}\frac{\pi}{2}.$$

3.

(a) Une intégration par parties donne pour $n \geq 1$:

$$\begin{aligned}I_n &= \int_0^{\frac{\pi}{2}} \cos^{2n}(t)\,dt = \left[t\cos^{2n}(t)\right]_0^{\frac{\pi}{2}} + 2n\int_0^{\frac{\pi}{2}} t\sin(t)\cos^{2n-1}(t)\,dt \\ &= 2n\int_0^{\frac{\pi}{2}} t\sin(t)\cos^{2n-1}(t)\,dt = 2nI'_n\end{aligned}$$

puis une deuxième intégration par parties donne :

$$\begin{aligned}I'_n &= \left[\frac{t^2}{2}\sin(t)\cos^{2n-1}(t)\right]_0^{\frac{\pi}{2}} \\ &\quad - \int_0^{\frac{\pi}{2}} \frac{t^2}{2}\left(\cos^{2n}(t) - (2n-1)\sin^2(t)\cos^{2n-2}(t)\right)dt \\ &= (2n-1)\int_0^{\frac{\pi}{2}} \frac{t^2}{2}\sin^2(t)\cos^{2n-2}(t)\,dt - \int_0^{\frac{\pi}{2}} \frac{t^2}{2}\cos^{2n}(t)\,dt \\ &= (2n-1)\int_0^{\frac{\pi}{2}} \frac{t^2}{2}\left(1-\cos^2(t)\right)\cos^{2n-2}(t)\,dt - \int_0^{\frac{\pi}{2}} \frac{t^2}{2}\cos^{2n}(t)\,dt \\ &= (2n-1)\int_0^{\frac{\pi}{2}} \frac{t^2}{2}\cos^{2n-2}(t)\,dt - n\int_0^{\frac{\pi}{2}} t^2\cos^{2n}(t)\,dt\end{aligned}$$

ce qui entraîne :

$$\begin{aligned} I_n &= n(2n-1)\int_0^{\frac{\pi}{2}} t^2\cos^{2n-2}(t)\,dt - 2n^2\int_0^{\frac{\pi}{2}} t^2\cos^{2n}(t)\,dt \\ &= n(2n-1)J_{n-1} - 2n^2 J_n. \end{aligned}$$

(b) On a :

$$\begin{aligned} K_{n-1} - K_n &= \frac{4^{n-1}\left((n-1)!\right)^2}{(2n)!}\left(2n(2n-1)J_{n-1} - 4n^2 J_n\right) \\ &= \frac{4^{n-1}\left((n-1)!\right)^2}{(2n)!}2I_n \\ &= \frac{4^{n-1}\left((n-1)!\right)^2}{(2n)!}2\frac{(2n)!}{4^n(n!)^2}\frac{\pi}{2} = \frac{\pi}{4n^2} \end{aligned}$$

(c) Il en résulte que :

$$\frac{\pi}{4}\sum_{k=1}^{n}\frac{1}{k^2} = \sum_{k=1}^{n}(K_{k-1} - K_k) = K_0 - K_n = J_0 - K_n.$$

4.

(a) La fonction sin étant convexe sur $\left[0, \frac{\pi}{2}\right]$, son graphe est au dessus de la corde d'extrémités $(0,0)$ et $\left(\frac{\pi}{2}, 1\right)$, ce qui se traduit par $\sin(x) \geq \frac{2}{\pi}x$.

(b) Pour tout $t \in \left[0, \frac{\pi}{2}\right]$, on a :

$$0 \leq t^2\cos^{2n}(t) \leq \frac{\pi^2}{4}\sin^2(t)\cos^{2n}(t) \leq \frac{\pi^2}{4}\left(1 - \cos^2(t)\right)\cos^{2n}(t)$$

et en intégrant :

$$0 \leq J_n \leq \frac{\pi^2}{4}(I_n - I_{n+1}) = \frac{\pi^2}{4}\left(1 - \frac{2n+1}{2n+2}\right)I_n = \frac{\pi^2 I_n}{8(n+1)}.$$

Tenant compte de $I_n = \frac{J_n}{K_n}\frac{\pi}{2}$, cela s'écrit :

$$0 \leq J_n \leq \frac{\pi^2}{8(n+1)}\frac{J_n}{K_n}\frac{\pi}{2}$$

soit :

$$0 \leq K_n \leq \frac{\pi^3}{16(n+1)}.$$

(c) De ce dernier encadrement, on déduit que $\lim\limits_{n\to+\infty} K_n = 0$ et avec III.3.c. on obtient :

$$\lim_{n\to+\infty} \frac{\pi}{4}\sum_{k=1}^{n}\frac{1}{k^2} = J_0 = \frac{\pi^3}{24}$$

et $\lim\limits_{n\to+\infty} \sum\limits_{k=1}^{n}\frac{1}{k^2} = \frac{\pi^2}{6}$.

– IV – Noyau de Dirichlet

1. Pour tout entier naturel k et tout réel x on a :

$$\sin\left(\frac{x}{2}\right)\cos(kx) = \frac{1}{2}\left(\sin\left(\left(k+\frac{1}{2}\right)x\right) - \sin\left(\left(k-\frac{1}{2}\right)x\right)\right),$$

ce qui entraîne pour $n \geq 1$:

$$\sin\left(\tfrac{x}{2}\right)\left(\tfrac{1}{2}+\sum_{k=1}^{n}\cos(kx)\right) = \frac{1}{2}\left(\sin\left(\tfrac{x}{2}\right)+\sum_{k=1}^{n}\left(\sin\left(\tfrac{2k+1}{2}x\right)-\sin\left(\tfrac{2k-1}{2}x\right)\right)\right)$$
$$= \frac{1}{2}\sin\left(\tfrac{2n+1}{2}x\right).$$

ce qui peut aussi s'écrire pour x non congru à 0 modulo 2π :

$$D_n(x) = \frac{1}{2}\frac{\sin\left(\frac{2n+1}{2}x\right)}{\sin\left(\frac{x}{2}\right)}$$

La fonction $\theta_p : t \mapsto \dfrac{\sin(pt)}{\sin(t)}$, pour tout entier p, se prolonge en fait par continuité sur $\mathbb{R}$, donc aussi $D_n(x) = \dfrac{1}{2}\theta_{2n+1}\left(\dfrac{x}{2}\right)$. En effet, l'ensemble $\mathbb{R}\setminus\mathbb{Z}\pi$ est stable par la translation $x \mapsto x+2\pi$ et la fonction θ_p est continue et 2π-périodique sur $\mathbb{R}\setminus\mathbb{Z}\pi$ comme quotient de deux fonctions continues et 2π-périodiques, le dénominateur ne s'annulant jamais sur $\mathbb{R}\setminus\mathbb{Z}\pi$. Pour k entier relatif et $x = k\pi + t$ avec t voisin de 0 on a :

$$\theta_p(x) = (-1)^{(p-1)k}\frac{\sin(pt)}{\sin(t)} \underset{t\to 0}{\backsim} (-1)^{(p-1)k}p.$$

On peut donc prolonger la fonction θ_p par continuité en tout point $k\pi$ avec $k \in \mathbb{Z}$ en posant $\theta_p(k\pi) = (-1)^{(p-1)k}p$. La fonction obtenue est bien continue et 2π-périodique sur $\mathbb{R}$.

2.

(a) Une intégration par parties donne pour $k \geq 1$:

$$\int_0^\pi x\cos(kx)\,dx = \left[\frac{x}{k}\sin(kx)\right]_0^\pi - \frac{1}{k}\int_0^\pi \sin(kx)\,dx$$
$$= \left[\frac{x}{k}\sin(kx) + \frac{1}{k^2}\cos(kx)\right]_0^\pi = \frac{(-1)^k - 1}{k^2}$$

(b) La fonction D_n se prolongeant par continuité en 0 avec $D_n(0) = \frac{2n+1}{2}$, l'intégrale L_n est bien définie. Les calculs précédents donnent :

$$L_n = \frac{\pi^2}{4} - \sum_{k=1}^{n}\frac{1}{k^2} + \sum_{k=1}^{n}\frac{(-1)^k}{k^2}.$$

3. La fonction f se prolonge par continuité sur $[-\pi, \pi]$ avec $f(0) = 2$. Elle est de classe $\mathcal{C}^1$ sur $]-\pi, \pi[\setminus\{0\}$ avec :

$$f'(x) = \frac{\sin\left(\frac{x}{2}\right) - \frac{x}{2}\cos\left(\frac{x}{2}\right)}{\sin^2\left(\frac{x}{2}\right)}$$

et un développement limité en 0 donne :

$$f'(x) = \frac{x}{6} + o(x)$$

donc $\lim_{x\to 0} f'(x) = 0$. On déduit alors du théorème des accroissements finis que f se prolonge en une fonction de classe $\mathcal{C}^1$ sur $[-\pi, \pi]$ avec $f'(0)$.

4. Une intégration par parties donne pour Φ de classe $\mathcal{C}^1$ sur $[0, \pi]$ et $\lambda > 0$:

$$\int_0^\pi \Phi(x)\sin(\lambda x)\,dx = \left[-\frac{\Phi(x)}{\lambda}\cos(\lambda x)\right]_0^\pi + \frac{1}{\lambda}\int_0^\pi \Phi'(x)\cos(\lambda x)\,dx$$

ce qui entraîne en notant respectivement M_0 et M_1 les bornes supérieures de Φ et Φ' sur $[0, \pi]$:

$$\left|\int_0^\pi \Phi(x)\sin(\lambda x)\,dx\right| \leq \frac{2M_0 + \pi M_1}{\lambda} \underset{\lambda\to+\infty}{\to} 0.$$

5.

(a) La question précédente appliquée à la fonction $\Phi = \frac{1}{2}f$ nous donne $\lim_{n\to+\infty} L_n = 0$.

(b) Et **IV.2.b.** donne :

$$\sum_{n=1}^{+\infty} \frac{1}{n^2} - \sum_{n=1}^{+\infty} \frac{(-1)^n}{n^2} = \frac{\pi^2}{4}$$

et avec $\sum_{n=1}^{+\infty} \frac{(-1)^{n+1}}{n^2} = \frac{1}{2} \sum_{n=1}^{+\infty} \frac{1}{n^2}$ (question **II.5.**), on déduit que $\sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}$.

Remarques

Pour comprendre un peu mieux la construction proposée dans cette partie **IV** on rappelle les définitions et résultats suivants.
On appelle opérateur de convolution sur l'espace $\mathcal{F}$ des fonctions continues et périodiques sur $\mathbb{R}$ toute application u_K définie sur $\mathcal{F}$ par :

$$\forall f \in \mathcal{F},\ \forall x \in \mathbb{R},\ u_K(f)(x) = \int_{-\pi}^{\pi} f(x-t)\, K(t)\, dt,$$

où K est une fonction appartenant à $\mathcal{F}$.
On note :

$$u_K(f) = f * K.$$

Il est facile de vérifier qu'un opérateur de convolution est un opérateur linéaire sur $\mathcal{F}$.
On a alors les résultats suivants.

Lemme 1 *Si K est une fonction appartenant à $\mathcal{F}$, alors pour toute fonction f appartenant à $\mathcal{F}$ on a :*

$$\forall x \in \mathbb{R},\ u_K(f)(x) = \int_{-\pi}^{\pi} f(t)\, K(x-t)\, dt.$$

Preuve : Le changement de variable $y = x - t$ donne :

$$u_K(f)(x) = \int_{x-\pi}^{x+\pi} f(y)\, K(x-y)\, dy.$$

Puis avec le changement de variable $z = y + 2\pi$ et la 2π-périodicité de la fonction $y \mapsto f(y)\, K(x-y)$ on déduit que :

$$\int_{x-\pi}^{-\pi} f(y)\, K(x-y)\, du = -\int_{\pi}^{x+\pi} f(z)\, K(x-z)\, dz$$

et $u_K(f)(x) = \int_{-\pi}^{\pi} f(y)\, K(x-y)\, dy.$

Lemme 2 *Si K est un polynôme trigonométrique, alors pour toute fonction f appartenant à $\mathcal{F}$, $u_K(f)$ est un polynôme trigonométrique.*

Preuve : Il suffit de considérer le cas où la fonction K est l'une des fonctions de base $c_k : x \mapsto \cos(kx)$ $(k \in \mathbb{N})$ ou $s_k : x \mapsto \sin(kx)$ $(k \in \mathbb{N} \setminus \{0\})$.
Pour $K = c_0$ on a $u_K(f)(x) = \displaystyle\int_{-\pi}^{\pi} f(t)\,dt$ pour tout réel x, c'est-à-dire que $u_K(f)$ est une fonction constante.
Pour tout entier k strictement positif et toute fonction f appartenant à $\mathcal{F}$ on a :

$$\left\{\begin{array}{lcl} u_{c_k}(f)(x) & = & \displaystyle\int_{-\pi}^{\pi} f(t)\,c_k(x-t)\,dt \\ & = & \left(\displaystyle\int_{-\pi}^{\pi} f(t)\,c_k(t)\,dt\right) c_k(x) + \left(\displaystyle\int_{-\pi}^{\pi} f(t)\,s_k(t)\,dt\right) s_k(x), \\ u_{s_k}(f)(x) & = & \displaystyle\int_{-\pi}^{\pi} f(t)\,s_k(x-t)\,dt \\ & = & -\left(\displaystyle\int_{-\pi}^{\pi} f(t)\,s_k(t)\,dt\right) c_k(x) + \left(\displaystyle\int_{-\pi}^{\pi} f(t)\,c_k(t)\,dt\right) s_k(x). \end{array}\right.$$

Pour toute fonction f appartenant à $\mathcal{F}$, on désigne par $(a_k(f))_{k\geq 0}$ et $(b_k(f))_{k\geq 1}$ les suites des coefficients de Fourier de f définis par :

$$\forall k \in \mathbb{N},\ a_k(f) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\cos(kt)\,dt = \frac{1}{\pi}(f * c_k)(0),$$
$$\forall k \in \mathbb{N}\setminus\{0\},\ b_k(f) = \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\sin(kt)\,dt = -\frac{1}{\pi}(f * s_k)(0).$$

On note $(S_n(f))_{n\geq 0}$ la suite des sommes de Fourier de la fonction f définie par :

$$\left\{\begin{array}{l} S_0(f) = \dfrac{a_0(f)}{2}c_0, \\ S_n(f) = \dfrac{a_0(f)}{2}c_0 + \sum\limits_{k=1}^{n}(a_k(f)\,c_k + b_k(f)\,s_k). \end{array}\right.$$

En remarquant que pour tout entier naturel k, on a :

$$f * c_k = \pi\,(a_k(f)\,c_k + b_k(f)\,s_k),$$

en posant $b_0(f) = 0$, les sommes de Fourier de f s'écrivent :

$$S_n(f) = \frac{1}{\pi}f * \left(\frac{1}{2}c_0 + \sum_{k=1}^{n} c_k\right) = \frac{1}{\pi}f * D_n.$$

Lemme 3 *Pour tout entier naturel n, on a :*

$$S_n(c_j) = \begin{cases} c_j \text{ si } 0 \leq j \leq n, \\ 0 \text{ si } j > n \geq 0, \end{cases} \quad S_n(s_j) = \begin{cases} s_j \text{ si } 1 \leq j \leq n, \\ 0 \text{ si } j > n \geq 0. \end{cases}$$

Preuve : Le calcul des $S_n(c_j)$ et $S_n(s_j)$ passe par le calcul des coefficients de Fourier des fonctions c_j et s_j.
Pour $k \in \mathbb{N}$ et $j \in \mathbb{N} \setminus \{0\}$ on a :

$$\begin{aligned} a_k(s_j) &= \frac{1}{\pi} \int_{-\pi}^{\pi} \sin(jt) \cos(kt)\, dt \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} (\sin((j+k)t) + \sin((j-k)t))\, dt = 0. \end{aligned}$$

De même pour $k \in \mathbb{N} \setminus \{0\}$ et $j \in \mathbb{N}$ on a :

$$b_k(c_j) = \frac{1}{\pi} \int_{-\pi}^{\pi} \cos(jt) \sin(kt)\, dt = 0.$$

Pour j, k dans $\mathbb{N}$ on a :

$$\begin{aligned} a_k(c_j) &= \frac{1}{\pi} \int_{-\pi}^{\pi} \cos(jt) \cos(kt)\, dt \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} (\cos((j-k)t) + \cos((j-k)t))\, dt = \begin{cases} 0 \text{ si } j \neq k, \\ 1 \text{ si } j = k \neq 0, \\ 2 \text{ si } j = k = 0. \end{cases} \end{aligned}$$

Pour j, k dans $\mathbb{N} \setminus \{0\}$ on a :

$$\begin{aligned} b_k(s_j) &= \frac{1}{\pi} \int_{-\pi}^{\pi} \sin(jt) \sin(kt)\, dt \\ &= \frac{1}{2\pi} \int_{-\pi}^{\pi} (\cos((j-k)t) - \cos((j-k)t))\, dt = \begin{cases} 0 \text{ si } j \neq k, \\ 1 \text{ si } j = k. \end{cases} \end{aligned}$$

On déduit alors que :

$$S_n(c_j) = \begin{cases} c_j \text{ si } 0 \leq j \leq n, \\ 0 \text{ si } j > n \geq 0, \end{cases} \quad S_n(s_j) = \begin{cases} s_j \text{ si } 1 \leq j \leq n, \\ 0 \text{ si } j > n \geq 0. \end{cases}$$

Pour tout entier naturel n, S_n est un opérateur linéaire défini sur $\mathcal{F}$ et à valeurs dans l'espace $\mathcal{P}_n$ des polynômes trigonométriques de degré au plus égal à n laissant invariant les éléments de $\mathcal{P}_n$. En fait S_n est l'opérateur de projection orthogonale de $\mathcal{F}$ sur $\mathcal{P}_n$.

Les opérateurs S_n sont appelés opérateurs de Fourier et les fonctions :

$$D_n = \frac{1}{2}c_0 + \sum_{k=1}^{n} c_k$$

sont appelées noyaux de Dirichlet.
On a donc, pour toute fonction f appartenant à $\mathcal{F}$:

$$\begin{aligned} S_n(f)(x) &= \frac{1}{\pi}(f * D_n)(x) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t) D_n(x-t)\,dt \\ &= \frac{a_0(f)}{2} + \sum_{k=1}^{n} (a_k(f)\cos(kx) + b_k(f)\sin(kx)). \end{aligned}$$

Cette formule étant également valable pour $n = 0$.
En désignant par f la fonction 2π-périodique définie par $f(t) = |t|$ sur $[-\pi, \pi]$, on a :

$$S_n(f)(0) = \frac{1}{2\pi}\int_{-\pi}^{\pi} f(t) D_n(-t)\,dt = \frac{1}{\pi}\int_{0}^{\pi} f(t) D_n(t)\,dt = \frac{1}{\pi}L_n$$

en utilisant la parité de f et de D_n.
Par ailleurs le théorème de Dirichlet nous dit que pour tout réel x, la suite $(S_n(f)(x))_{n\geq 1}$ converge vers f (la fonction f est continue et $\mathcal{C}^1$ par morceaux sur $\mathbb{R}$) et donc :

$$\lim_{n\to+\infty} L_n = \pi \lim_{n\to+\infty} S_n(f)(0) = f(0) = 0$$

avec :

$$S_n(f)(0) = \frac{a_0(f)}{2} + \sum_{k=1}^{n} a_k(f)$$

les coefficients $a_k(f)$ étant donnés par :

$$\begin{aligned} a_k(f) &= \frac{1}{\pi}\int_{-\pi}^{\pi} f(t)\cos(kt)\,dt = a_k(f) \\ &= \frac{2}{\pi}\int_{0}^{\pi} t\cos(kt)\,dt = \frac{(-1)^k - 1}{k^2} \end{aligned}$$

– V – Une somme double

1.

(a) La fonction $t \rightarrow \dfrac{1}{t}$ étant décroissante sur $\mathbb{R}^{+*}$, on a :

$$\forall k \geq 1,\ \frac{1}{k+1} \leq \int_k^{k+1} \frac{dt}{t} \leq \frac{1}{k}$$

et pour tout $N \geq 1$, on a :

$$H_N = \sum_{k=1}^{N} \frac{1}{k} \geq \sum_{k=1}^{N} \int_k^{k+1} \frac{dt}{t} = \int_1^{N+1} \frac{dt}{t} = \ln(N+1).$$

Pour $N \geq 2$, on a :

$$\begin{aligned} H_N = 1 + \sum_{k=2}^{N} \frac{1}{k} = 1 + \sum_{k=1}^{N-1} \frac{1}{k+1} \\ \leq 1 + \sum_{k=1}^{N-1} \int_k^{k+1} \frac{dt}{t} = 1 + \int_1^{N} \frac{dt}{t} = 1 + \ln(N) \end{aligned}$$

Pour $N = 1$, on a $H_1 = 1 + \ln(1)$.

(b) L'encadrement précédent s'écrit aussi :

$$\frac{\ln(N+1)}{N} \leq \frac{H_N}{N} \leq \frac{1+\ln(N)}{N}$$

et faisant tendre N vers l'infini, on en déduit que $\lim\limits_{N \rightarrow +\infty} H_N = 0$.

(c) Avec $\dfrac{1}{m(m+1)} = \dfrac{1}{m} - \dfrac{1}{m+1}$, on obtient :

$$\begin{aligned} \sum_{m=1}^{M-1} \frac{H_m}{m(m+1)} = \sum_{m=1}^{M-1} \frac{H_m}{m} - \sum_{m=1}^{M-1} \frac{H_m}{m+1} = \sum_{m=1}^{M-1} \frac{H_m}{m} - \sum_{m=2}^{M} \frac{H_{m-1}}{m} \\ = 1 + \sum_{m=2}^{M-1} \frac{H_m - H_{m-1}}{m} - \frac{H_{M-1}}{M} \\ = 1 + \sum_{m=2}^{M} \frac{H_m - H_{m-1}}{m} - \frac{H_M}{M} \end{aligned}$$

avec $H_m - H_{m-1} = \frac{1}{m}$, ce qui donne :

$$\sum_{m=1}^{M-1} \frac{H_m}{m(m+1)} = \sum_{m=1}^{M} \frac{1}{m^2} - \frac{H_M}{M}.$$

(d) Il en résulte que :

$$\sum_{m=1}^{+\infty} \frac{H_m}{m(m+1)} = \sum_{m=1}^{+\infty} \frac{1}{m^2} - \lim_{M \to +\infty} \frac{H_M}{M} = \frac{\pi^2}{6}.$$

2.

(a) Avec $\frac{1}{n(n+m-1)} = \frac{1}{m-1}\left(\frac{1}{n} - \frac{1}{n+m-1}\right)$ pour $m \geq 2$ et $n \geq 1$, on obtient :

$$\begin{aligned} Z_{N,m} &= \frac{1}{m-1}\left(\sum_{n=1}^{N} \frac{1}{n} - \sum_{n=1}^{N} \frac{1}{n+m-1}\right) \\ &= \frac{1}{m-1}\left(\sum_{n=1}^{N} \frac{1}{n} - \sum_{n=m}^{N+m-1} \frac{1}{n}\right) \\ &= \frac{1}{m-1}\left(H_N - (H_{N+m-1} - H_{m-1})\right) \\ &= \frac{1}{m-1}\left(H_{m-1} - (H_{N+m-1} - H_N)\right) \end{aligned}$$

soit :

$$Z_{N,m} = \frac{1}{m-1}\left(H_{m-1} - \sum_{n=N+1}^{N+m-1} \frac{1}{n}\right).$$

(b) Pour $m \geq 2$ fixé et $N \geq 1$, on a :

$$0 \leq \sum_{n=N+1}^{N+m-1} \frac{1}{n} \leq (m-1)\frac{1}{N+1} \underset{N \to +\infty}{\to} 0$$

et en conséquence $\lim_{N \to +\infty} Z_{N,m} = \frac{H_{m-1}}{m-1}$.

3.

(a) Pour $N \geq 1$ et $M \geq 2$, on a :

$$\sum_{n=1}^{N}\sum_{m=1}^{M}\frac{1}{nm\,(n+m-1)} = \sum_{m=1}^{M}\frac{1}{m}\sum_{n=1}^{N}\frac{1}{n\,(n+m-1)} = \sum_{m=1}^{M}\frac{1}{m}Z_{N,m} = Z_{N,1} + \sum_{m=2}^{M}\frac{1}{m}Z_{N,m}$$

avec :

$$Z_{N,1} = \sum_{n=1}^{N}\frac{1}{n^2}$$

(b) Avec $\lim\limits_{N\to+\infty} Z_{N,m} = \dfrac{H_{m-1}}{m-1}$, on déduit alors que :

$$\lim_{N\to+\infty}\left(\sum_{n=1}^{N}\sum_{m=1}^{M}\frac{1}{nm\,(n+m-1)}\right) = \frac{\pi^2}{6} + \sum_{m=2}^{M}\frac{H_{m-1}}{m\,(m-1)} = \frac{\pi^2}{6} + \sum_{m=1}^{M-1}\frac{H_m}{m\,(m+1)}$$

(c) Avec $\displaystyle\sum_{m=1}^{+\infty}\frac{H_m}{m\,(m+1)} = \frac{\pi^2}{6}$, on en déduit que :

$$\lim_{M\to+\infty}\left(\lim_{N\to+\infty}\left(\sum_{n=1}^{N}\sum_{m=1}^{M}\frac{1}{nm\,(n+m-1)}\right)\right) = \frac{\pi^2}{3}.$$

– VI – La fonction Dilogarithme

1. La fonction $f : t \mapsto \dfrac{\ln(1-t)}{t}$ est indéfiniment dérivable sur $]-\infty, 1[\setminus\{0\}$ avec :

$$\lim_{t\to 0}\frac{\ln(1-t)}{t} = \lim_{x\to 1}\frac{\ln(x)-\ln(1)}{1-x} = -\ln'(1) = -1$$

elle se prolonge donc par continuité en 0 et la fonction L_i est bien définie sur $]-\infty, 1[$. Sur cet intervalle, elle est $\mathcal{C}^\infty$ avec $L_i'(x) = -\dfrac{\ln(1-x)}{x}$.

2. Il s'agit de montrer la convergence de l'intégrale impropre $\int_0^1 \frac{\ln(1-t)}{t}dt$.

   Au voisinage de 1, on a $\left|\frac{\ln(1-t)}{t}\right| \backsim |\ln(1-t)| = -\ln(1-t)$ avec :

$$\begin{aligned}\int_0^x \ln(1-t)\,dt &= \int_{1-x}^1 \ln(u)\,du = [u\ln(u)-u]_{1-x}^1 \\ &= -1-(1-x)\ln(1-x)+(1-x) \underset{x\to 1}{\to} -1\end{aligned}$$

   Il en résulte que l'intégrale $\int_0^1 \frac{\ln(1-t)}{t}dt$ est absolument convergente, ce qui permet de prolonger L_i par continuité en 1 en posant $L_i(1) = -\int_0^1 \frac{\ln(1-t)}{t}dt$.

3.

   (a) Pour tout $t \in \left]-1,1\right[$, on a :

$$\frac{\ln(1-t)}{t} = -\sum_{n=1}^{+\infty}\frac{t^{n-1}}{n}$$

   la convergence étant uniforme sur tout segment $[-r,r]$ pour $r \in \left[0,1\right[$. On peut donc intégrer terme à terme pour écrire, pour tout $x \in \left]-1,1\right[$:

$$L_i(x) = \sum_{n=1}^{+\infty}\int_0^x \frac{t^{n-1}}{n} = \sum_{n=1}^{+\infty}\frac{x^n}{n^2}.$$

   (b) La série $\sum \frac{x^n}{n^2}$ étant normalement convergente sur $[-1,1]$, sa somme $g(x)$ est continue sur cet intervalle et avec la continuité de L_i en 1, on peut écrire que :

$$\begin{aligned}L_i(1) = \lim_{x\to 1^-} L_i(x) &= \lim_{x\to 1^-} g(x) = g(1) \\ &= \sum_{n=1}^{+\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.\end{aligned}$$

   De même, on a :

$$L_i(-1) = g(-1) = \sum_{n=1}^{+\infty}\frac{(-1)^n}{n^2} = -\frac{\pi^2}{12}.$$

4.

(a) La fonction L_i étant de classe $\mathcal{C}^\infty$ sur $]-\infty, 1[$, la fonction $f : x \mapsto L_i(x) + L_i(1-x)$ est de classe $\mathcal{C}^\infty$ sur $]0, 1[$ avec

$$f'(x) = -\frac{\ln(1-x)}{x} + \frac{\ln(x)}{1-x}.$$

(b) En remarquant que :

$$f'(x) = -(\ln(1-x)\ln(x))'$$

sur l'intervalle $]0, 1[$, on déduit que :

$$f(x) = -\ln(1-x)\ln(x) + \alpha$$

où la constante α est donnée par

$$\alpha = \lim_{x \to 0^+} (f(x) + \ln(1-x)\ln(x)) = L_i(1) = \frac{\pi^2}{6}.$$

On a donc :

$$f(x) = L_i(x) + L_i(1-x) = \frac{\pi^2}{6} - \ln(1-x)\ln(x)$$

pour tout $x \in]0, 1[$.

5. Prenant $x = \dfrac{1}{2}$ dans l'égalité précédente, on obtient :

$$L_i\left(\frac{1}{2}\right) = \sum_{n=1}^{+\infty} \frac{1}{2^n}\frac{1}{n^2} = \frac{1}{2}\left(\frac{\pi^2}{6} - \ln^2\left(\frac{1}{2}\right)\right) = \frac{\pi^2}{12} - \frac{\ln^2(2)}{2}.$$

6.

(a) Les fonctions $L_i(x) + L_i(-x)$ et $\dfrac{1}{2}L_i(x^2)$ ayant même dérivée $-\dfrac{\ln(1-x^2)}{x}$ sur l'intervalle $]-1, 1[$ et prenant la même valeur en 0, sont identiques.

(b) L'égalité précédente s'écrit aussi, pour $x \in]-1, 1[$:

$$\sum_{n=1}^{+\infty} \frac{x^n}{n^2} + \sum_{n=1}^{+\infty} \frac{(-1)^n x^n}{n^2} = \frac{1}{2}\sum_{n=1}^{+\infty} \frac{x^{2n}}{n^2}$$

Toutes ces expressions étant continues sur $[-1, 1]$ (convergence normale des séries), on peut les évaluer en $x = 1$ et on retrouve :

$$\sum_{n=1}^{+\infty} \frac{(-1)^n x^n}{n^2} = -\frac{1}{2}\sum_{n=1}^{+\infty} \frac{x^{2n}}{n^2} = -\frac{\pi^2}{12}.$$

7.

(a) La fonction L_i étant de classe $\mathcal{C}^\infty$ sur $]-\infty, 1[$, la fonction :

$$f : x \mapsto L_i(x) - L_i(-x)$$

est de classe $\mathcal{C}^\infty$ sur $]-1, 1[$ avec :

$$f'(x) = -\frac{\ln(1-x)}{x} + \frac{\ln(1+x)}{x} = \frac{1}{x}\ln\left(\frac{1+x}{1-x}\right).$$

La fonction $x \mapsto \dfrac{1-x}{1+x}$ étant de classe $\mathcal{C}^\infty$ de $]0, 1[$ sur $]0, 1[$, la fonction :

$$g : x \mapsto L_i\left(\frac{1-x}{1+x}\right) - L_i\left(\frac{x-1}{1+x}\right) = f\left(\frac{1-x}{1+x}\right)$$

est de classe $\mathcal{C}^\infty$ sur $]0, 1[$ avec :

$$g'(x) = -\frac{2}{(1+x)^2} f'\left(\frac{1-x}{1+x}\right) = -\frac{2}{(1+x)^2}\frac{1+x}{1-x}\ln\left(\frac{1+\frac{1-x}{1+x}}{1-\frac{1-x}{1+x}}\right)$$
$$= -\frac{2}{1-x^2}\ln\left(\frac{2}{2x}\right) = \frac{2}{1-x^2}\ln(x).$$

Si on considère la fonction :

$$h : x \mapsto \ln\left(\frac{1+x}{1-x}\right)\ln(x)$$

on constate que cette fonction est de classe $\mathcal{C}^\infty$ sur $]0, 1[$ avec :

$$h'(x) = \frac{1}{x}\ln\left(\frac{1+x}{1-x}\right) + \frac{2}{1-x^2}\ln(x) = f'(x) + g'(x).$$

On a donc sur $]0, 1[$:

$$f(x) + g(x) = h(x) + \alpha$$

et avec :

$$\lim_{x\to 0^+} f(x) + g(x) = L_i(1) - L_i(-1) = \frac{\pi^2}{6} + \frac{\pi^2}{12} = \frac{\pi^2}{4}$$

$$\lim_{x\to 0^+} h(x) = \lim_{x\to 0^+} \ln\left(\frac{1+x}{1-x}\right)\ln(x) = \lim_{x\to 0^+} 2x\ln(x) = 0$$

(un développement limité donne $\ln\left(\frac{1+x}{1-x}\right) = 2x + o(x)$), on déduit que $\alpha = \frac{\pi^2}{4}$ et :

$$L_i(x) - L_i(-x) + L_i\left(\frac{1-x}{1+x}\right) - L_i\left(\frac{x-1}{1+x}\right) = \frac{\pi^2}{4} + \ln\left(\frac{1+x}{1-x}\right)\ln(x).$$

(b) En utilisant le développement en série entière sur $]-1,1[$:

$$L_i(x) = \sum_{n=1}^{+\infty} \frac{x^n}{n^2}$$

on obtient sur $]0,1[$:

$$f(x) = L_i(x) - L_i(-x) = 2\sum_{n=1}^{+\infty} \frac{x^{2n+1}}{(2n+1)^2}$$

$$L_i\left(\frac{1-x}{1+x}\right) - L_i\left(\frac{x-1}{1+x}\right) = 2\sum_{n=1}^{+\infty} \frac{1}{(2n+1)^2}\left(\frac{1-x}{1+x}\right)^{2n+1}$$

et :

$$\frac{\pi^2}{4} + \ln\left(\frac{1+x}{1-x}\right)\ln(x) = 2\sum_{n=1}^{+\infty} \frac{1}{(2n+1)^2}\left(x^{2n+1} + \left(\frac{1-x}{1+x}\right)^{2n+1}\right)$$

On cherche alors $x \in]0,1[$ tel que $\frac{1-x}{1+x} = x$, ce qui donne $x^2 + 2x - 1 = 0$ et $x = \sqrt{2} - 1$. Ce qui donne :

$$\sum_{n=1}^{+\infty} \frac{\left(\sqrt{2}-1\right)^{2n+1}}{(2n+1)^2} = \frac{\pi^2}{16} - \frac{\ln^2\left(\sqrt{2}-1\right)}{4}.$$

Chapitre 3

CAPES externe 2008, épreuve 1

3.1 Énoncé

Fonctions à variations bornées

Introduction

Dans ce problème, on s'intéresse aux fonctions à variations bornées. Cette notion a été introduite en 1881 par Jordan[1] pour étendre un théorème de Dirichlet[2] sur la convergence des séries de Fourier[3]. Il est composé de sept parties **A**, **B**, **C**, **D**, **E**, **F** et **G**.
Dans la partie **A** on établit quelques propriétés élémentaires relatives aux fonctions à variations bornées.
En introduction de la partie **B**, on définit une notion de longueur bornée et de longueur pour les fonctions à valeurs dans $\mathbb{R}$. Son objectif est d'établir des propriétés générales sur cette notion : une inégalité triangulaire, une relation de Chasles ...
Dans la partie **C** on établit l'équivalence entre « être de longueur bornée sur tout segment » et « être à variations bornées ».
La partie **D** se consacre au cas des fonctions de classe $\mathcal{C}^1$. On y démontre qu'elles sont toujours de longueur bornée et on donne une formule pour calculer leur longueur.
La partie **E** s'intéresse au cas des fonctions périodiques. La partie **F** est consacrée à l'étude d'un exemple.

[1] Camille Marie Ennenmond Jordan, mathématicien français, Lyon 1838 – Paris 1922.
[2] Gustav Peter Dirichlet, mathématicien allemand, Düren 1805 – Göttingen 1859.
[3] Joseph Jean-Baptiste Fourier, mathématicien français, Auxerre 1768 – Paris 1830.

Dans la partie **G**, on étend les définitions et les propriétés présentées précédemment aux cas des fonctions à valeurs dans $\mathbb{R}^n$.
Sauf mentions contraires explicitées dans le texte, les parties de ce sujet ne sont pas a priori indépendantes.

Notations et définitions

- Pour $n \in \mathbb{N}^*$ et $A \subseteq \mathbb{R}$, $\mathcal{F}(A, \mathbb{R}^n)$ désigne l'ensemble des fonctions de A vers $\mathbb{R}^n$. Pour tout $f \in \mathcal{F}(A, \mathbb{R}^n)$ et $B \subseteq A$, $f|_B$ désigne la restriction de f à B.
- Dans tout le problème, I désignera un intervalle de $\mathbb{R}$ non vide et non réduit à un point.
- Pour $f \in \mathcal{F}(I, \mathbb{R})$, on dit que f est à variations bornées lorsqu'il existe $g \in \mathcal{F}(I, \mathbb{R})$ croissante et $h \in \mathcal{F}(I, \mathbb{R})$ décroissante telles que $f = g + h$.

– A – Premières propriétés

A1 Établir que toute fonction monotone définie sur I est à variations bornées.

A2a Montrer que l'ensemble des fonctions à variations bornées définies sur I est un sous-espace vectoriel de $\mathcal{F}(I, \mathbb{R})$.

A2b Établir que ce sous-espace est engendré par l'ensemble des fonctions croissantes sur I.

Dans la fin de cette partie, on considère $f \in \mathcal{F}(I, \mathbb{R})$ une fonction à variations bornées, et a et b deux éléments de I tels que $a < b$.

A3 Soit $\alpha \in I$. Démontrer qu'il existe $k \in \mathcal{F}(I, \mathbb{R})$ croissante et $\ell \in \mathcal{F}(I, \mathbb{R})$ décroissante telles que $f = k + \ell$ et $k(\alpha) = 0$.

A4 On écrit $f = g+h$ avec g croissante sur I et h décroissante sur I. Prouver que :

$$g(b) - g(a) \geqslant f(b) - f(a) \geqslant h(b) - h(a).$$

A5 Montrer que f est bornée sur le segment $[a, b]$.

A6 Établir qu'en tout point intérieur à I, la fonction f admet une limite à droite et une limite à gauche.

– B – Fonctions de longueur bornée

Soient a et b dans I avec $a < b$ et $f \in \mathcal{F}(I, \mathbb{R})$. On rappelle qu'une subdivision σ de $[a, b]$ est une suite finie, strictement croissante, qu'on peut noter $(\sigma_k)_{0 \ \ k \ \ p}$ où $p \in \mathbb{N}^*$, et vérifiant $\sigma_0 = a$ et $\sigma_p = b$.
Pour $\sigma = (\sigma_k)_{0 \ \ k \ \ p}$ une subdivision de $[a, b]$ avec $p \in \mathbb{N}^*$, on pose :

$$\ell(\sigma, f) = \sum_{i=1}^{i=p} |f(\sigma_i) - f(\sigma_{i-1})|.$$

On dit que f est de longueur bornée sur le segment $[a, b]$ lorsqu'il existe $\Lambda \in \mathbb{R}$ tel que pour tout σ subdivision de $[a, b]$ on ait $\ell(\sigma, f) < \Lambda$. Si f est de longueur bornée sur $[a, b]$, on définit alors $L_a^b(f)$, la longueur de a à b de f, par :

$$L_a^b(f) = \sup_{\sigma}\{\, \ell(\sigma, f) \mid \sigma \text{ est une subdivision de } [a, b]\}.$$

De plus, on pose également $L_b^a(f) = -L_a^b(f)$ et $L_a^a(f) = 0$.
Dans cette partie, on considère f et g dans $\mathcal{F}(I, \mathbb{R})$ et a, b, c trois éléments de I tels que $a < c < b$.

B1 On suppose que f est de longueur bornée sur $[a, b]$. Montrer que :

$$L_a^b(f) \geqslant 0.$$

B2 On suppose que f est de longueur bornée sur $[a, b]$. Montrer que :

$$|f(b) - f(a)| \leqslant L_a^b(f).$$

B3 On suppose que f et g sont de longueur bornée sur $[a, b]$. Établir que $f + g$ est de longueur bornée sur $[a, b]$ et que :

$$L_a^b(f + g) \leqslant L_a^b(f) + L_a^b(g).$$

B4 On suppose que f est de longueur bornée sur $[a, c]$ et sur $[c, b]$. On considère une subdivision $\sigma = (\sigma_k)_{0 \ \ k \ \ p}$ de $[a, b]$ et on pose :

$$\begin{cases} q = \max\{j \in \{0, \cdots, p\} \mid \sigma_j < c\} \\ r = \min\{j \in \{0, \cdots, p\} \mid \sigma_j > c\} \end{cases}$$

B4a Justifier l'existence de q et de r.

On définit alors les suites finies σ' et σ'' par :

$$\begin{cases} \sigma'_j = \sigma_j \text{ si } j \in \{0, \cdots, q\} \\ \sigma'_{q+1} = c \end{cases}$$

$$\begin{cases} \sigma''_0 = c \\ \sigma''_j = \sigma_{j+r-1} \text{ si } j \in p - r + 1 \end{cases}$$

B4b Montrer que σ' est une subdivision de $[a, c]$ et que σ'' est une subdivision de $[c, b]$.

B4c Montrer que $\ell(\sigma, f) \leqslant \ell(\sigma', f) + \ell(\sigma'', f)$.

B4d Prouver que f est de longueur bornée sur $[a, b]$ et que :

$$L_a^b(f) \leq L_a^c(f) + L_c^b(f).$$

B5 On suppose maintenant que f est de longueur bornée sur $[a, b]$ et on considère une subdivision quelconque σ' de $[a, c]$ et une subdivision quelconque σ'' de $[c, b]$.

B5a Démontrer qu'il existe une subdivision de $[a, b]$, notée σ, telle qu'on ait :

$$\ell(\sigma, f) = \ell\left(\sigma', f\right) + \ell\left(\sigma'', f\right).$$

B5b Montrer que f est de longueur bornée sur $[a, c]$ et sur $[c, b]$ et que :

$$L_a^b(f) \geq L_a^c(f) + L_c^b(f).$$

B6 On suppose maintenant que f est de longueur bornée sur tout segment de I. Soient α, β, γ dans I, établir l'égalité :

$$L_\alpha^\beta(f) + L_\beta^\gamma(f) = L_\alpha^\gamma(f).$$

– C – Lien entre « être de longueur bornée » et « être à variations bornées »

On considère $f \in \mathcal{F}(I, \mathbb{R})$.

C1 Soient a et b dans I avec $a < b$.

C1a Soit $q \in \mathcal{F}(I, \mathbb{R})$ une fonction monotone. Prouver que q est de longueur bornée sur $[a, b]$ et qu'on a :

$$L_a^b(q) = |q(b) - q(a)|.$$

C1b On suppose que f est une fonction à variations bornées. Montrer que f est de longueur bornée sur $[a, b]$.

C2 On suppose que f est de longueur bornée sur tout segment de I. On choisit λ dans I et on définit alors les fonctions g et h, pour tout $t \in I$, par :

$$g(t) = \frac{1}{2}\left(f(t) + L_\lambda^t(f)\right) \text{ et } h(t) = \frac{1}{2}\left(f(t) - L_\lambda^t(f)\right)$$

Prouver que g est croissante sur I et que h est décroissante sur I.

C3 En déduire que f est à variations bornées si et seulement si f est de longueur bornée sur tout segment de I.

– D – Cas des fonctions de classe $\mathcal{C}^1$

On considère une fonction $f \in \mathcal{F}(I, \mathbb{R})$ de classe C^1 sur I. Le but de cette partie est de montrer que f est de longueur bornée sur tout segment de I et que pour tous α et β dans I on a :

$$L_\alpha^\beta(f) = \int_\alpha^\beta |f'(t)| dt.$$

D1 Soient u et v dans I avec $u < v$, établir que :

$$|f(u) - f(v)| \leqslant \int_u^v |f'(t)|\, dt.$$

D2 Soient a et b dans I avec $a < b$.

D2a Soit σ une subdivision de $[a, b]$. Établir que :

$$\ell(\sigma, f) \leqslant \int_a^b |f'(t)|\, dt.$$

D2b Démontrer que f est de longueur bornée sur $[a, b]$ et que :

$$L_a^b(f) \leqslant \int_a^b |f'(t)| dt.$$

D3 Soient a et b dans I avec $a < b$ et soit un réel $\varepsilon > 0$.

D3a Montrer qu'il existe $p \in \mathbb{N}^*$ et $\sigma = (\sigma_k)_{0 \quad k \quad p}$ une subdivision de $[a, b]$, tels que pour tout $i \in \{1, \cdots, p\}$ et pour tout x et y éléments de $[\sigma_{i-1}, \sigma_i]$ on ait :

$$|f'(x) - f'(y)| < \frac{\varepsilon}{b - a}.$$

D3b Prouver que pour tout $i \in \{1, \cdots, p\}$ il existe $c_i \in [\sigma_{i-1}, \sigma_i]$ tel que :

$$|f'(c_i)|(\sigma_i - \sigma_{i-1}) = |f(\sigma_i) - f(\sigma_{i-1})|.$$

D3c En déduire que pour tout $i \in \{1, \cdots, p\}$, on a :

$$|f(\sigma_i) - f(\sigma_{i-1})| \geqslant \int_{\sigma_{i-1}}^{\sigma_i} |f'(t)|dt - \frac{\varepsilon(\sigma_i - \sigma_{i-1})}{b-a}.$$

D3d Établir que

$$\ell(\sigma, f) \geqslant \int_a^b |f'(t)|dt - \varepsilon.$$

D4 Conclure.

D5 Établir que f est à variations bornées.

– E – Cas des fonctions périodiques

Dans cette partie on s'intéresse aux fonctions périodiques à variations bornées. On y utilise certains résultats de la partie **A.** Par ailleurs, les résultats de cette partie ne sont pas utilisés dans les autres parties.
Pour $x \in \mathbb{R}$, on note $[x]$ la partie entière de x. On rappelle que $[x]$ est l'unique élément de $\mathbb{Z}$ vérifiant :

$$[x] \leqslant x < [x] + 1.$$

On rappelle également que la fonction partie entière est croissante. On considère $T \in \mathbb{R}_+^*$ et on définit la fonction p sur $\mathbb{R}$ par $p(x) = \left[\frac{x}{T}\right]$.

E1 Pour tout $x \in \mathbb{R}$, montrer que $x - p(x)T \in [0, T[$.

E2 Pour a et b deux réels tels que $a \leqslant b$, établir que :

$$p(a) = p(b) \text{ ou } p(a) + 1 \leqslant p(b).$$

E3 Soit $f \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ une fonction périodique de période T. On suppose que $f|_{[0,T]}$ est à variations bornées. On peut donc écrire $f|_{[0,T]} = k + \ell$ avec $k \in \mathcal{F}([0,T], \mathbb{R})$ croissante, $\ell \in \mathcal{F}([0,T], \mathbb{R})$ décroissante et $k(0) = 0$ (d'après **A3**). Pour $x \in \mathbb{R}$, on pose :

$$g(x) = p(x)k(T) + k(x - p(x)T)$$
$$h(x) = f(x) - g(x).$$

E3a Justifier que les fonctions g et h sont bien définies sur $\mathbb{R}$.

E3b Soient a et b deux réels tels que $a \leqslant b$. Montrer que $g(a) \leqslant g(b)$.

E3c Montrer que pour tout réel x on a : $h(x) = -p(x)k(T) + \ell(x - p(x)T)$.

E3d Montrer que pour tout $u \in [0, T]$ on a $\ell(0) \geqslant \ell(u) \geqslant \ell(0) - k(T)$.

E3e Prouver finalement que f est à variations bornées.

E4 On considère la fonction

$$\psi : x \longmapsto \frac{1}{x - [x] - 1}$$

E4a Montrer que ψ est bien définie sur $\mathbb{R}$ et est périodique de période 1.

E4b Parmi les trois fonctions $\psi|_{[0,1[}, \psi|_{[0,1]}$ et ψ, quelles sont celles qui sont à variations bornées ? On justifiera chacune des réponses.

Dans la fin de cette partie, on considère la fonction φ définie, pour $x \in \mathbb{R}$, par :

$$\varphi(x) = |\sin x| + \sin x.$$

E5 Donner, sans justification, la représentation graphique de $\varphi|_{[-2\pi,2\pi]}$ dans un repère qu'on choisira.

E6 Montrer que φ est à variations bornées.

E7 D'après **A3** et **E6**, on peut écrire $\varphi = g + h$ avec $g \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ croissante vérifiant $g(0) = 0$ et $h \in \mathcal{F}(\mathbb{R}, \mathbb{R})$ décroissante.

E7a Établir que l'on a : $\forall n \in \mathbb{N},\ g(2n\pi) + 2 \leqslant g\left(2n\pi + \dfrac{\pi}{2}\right)$.

(Indication : On pourra utiliser **A4.**)

E7b En déduire que l'on a : $\forall n \in \mathbb{N},\ g(n\pi) \geqslant n$.

E7c Que vaut $\lim\limits_{x \to +\infty} g(x)$?

E7d En déduire $\lim\limits_{x \to +\infty} h(x)$.

– F – Un exemple de fonction dérivable et bornée, mais non à variations bornées

Les premières questions de cette partie peuvent se traiter indépendamment des parties précédentes.

On étudie dans cette partie certaines propriétés de la fonction f définie pour $x \in \mathbb{R}$ par :

$$\begin{cases} f(x) = x^2 \sin\left(\dfrac{1}{x^2}\right) \text{ si } x \neq 0 \\ f(0) = 0 \end{cases}$$

F1a Étudier la parité de f.

F1b Montrer que f est dérivable sur $\mathbb{R}$ et calculer $f'(x)$ pour tout x réel.

F1c La fonction f est-elle de classe $\mathcal{C}^1$ sur $\mathbb{R}$?

F1d Que vaut $\lim\limits_{x \to +\infty} f(x)$?

F1e En déduire que f est bornée.

F2 Montrer que la série de terme général $\ln\left(\dfrac{4n+1}{4n-1}\right)$ $(n \geqslant 1)$ est divergente.

F3 On considère la suite $(u_n)_{n\ \ 1}$ définie par $u_n = \sqrt{\dfrac{2}{(2n-1)\pi}}$

F3a Vérifier que la suite $(u_n)_{n\ \ 1}$ est décroissante et est de limite nulle.

F3b Soit $n \in \mathbb{N}^*$. Établir que

$$\int_{u_{n+1}}^{u_n} \frac{1}{t}\left|\cos\frac{1}{t^2}\right| dt \geqslant \frac{\sqrt{2}}{2}\int_{\sqrt{\frac{4}{(4n+1)\pi}}}^{\sqrt{\frac{4}{(4n-1)\pi}}} \frac{1}{t}dt.$$

F3c Prouver alors que la série de terme général $\displaystyle\int_{u_{n+1}}^{u_n} \frac{1}{t}\left|\cos\frac{1}{t^2}\right| dt$ $(n \geqslant 1)$ est divergente.

F3d En déduire que l'intégrale $\displaystyle\int_0^{u_1} \frac{1}{t}\left|\cos\frac{1}{t^2}\right| dt$ est divergente.

F4a Montrer que l'intégrale $\displaystyle\int_0^1 f'(t)\,dt$ est convergente mais qu'elle n'est pas absolument convergente.

F4b Que vaut $\displaystyle\lim_{x \to 0^+} \int_x^1 |f'(t)|\,dt$?

F5 Soient a et b deux réels tels que $a < b$ et $ab \leqslant 0$. Prouver que f n'est pas de longueur bornée sur $[a, b]$.

F6 Soit J un intervalle de $\mathbb{R}$ non vide et non réduit à un point. Démontrer que l'application $f|_J$ est à variations bornées si et seulement si $0 \notin J$.

– G – Généralisation au cas des fonctions à valeurs dans $\mathbb{R}^n$

Dans cette partie, on considère un entier $n \geqslant 2$ et on munit $\mathbb{R}^n$ de sa structure euclidienne canonique ; la norme euclidienne $\|\cdot\|$ associée est donc définie, pour $x = (x_1, \cdots, x_n) \in \mathbb{R}^n$, par :

$$\|x\| = \sqrt{\sum_{i=1}^{i=n} x_i^2}.$$

On peut prolonger la définition introduite au début de la partie **B**, de fonction de longueur bornée aux fonctions à valeurs dans $\mathbb{R}^n$ de la manière suivante : Etant données a et b dans I avec $a < b$ et $f \in \mathcal{F}(I, \mathbb{R}^n)$, pour $\sigma = (\sigma_k)_{0 \quad k \quad p}$ une subdivision de $[a, b]$ avec $p \in \mathbb{N}^*$, on pose :

$$\ell(\sigma, f) = \sum_{i=1}^{i=p} \| f(\sigma_i) - f(\sigma_{i-1}) \| .$$

On dit que f est de longueur bornée sur le segment $[a, b]$ lorsqu'il existe $\Lambda \in \mathbb{R}$ tel que pour tout σ subdivision de $[a, b]$ on ait $\ell(\sigma, f) < \Lambda$. Si f est de longueur bornée sur $[a, b]$, on définit alors $L_a^b\,(f)$, la longueur de a à b de f, par :

$$L_a^b(f) = \sup_\sigma \{\, \ell(\sigma, f) \mid \sigma \text{ est une subdivision de } [a, b]\,\}.$$

De plus, on pose également $L_b^a\,(f) = -L_a^b(f)$ et $L_a^a(f) = 0$.
Dans cette partie, on considère deux éléments a et b de I tels que $a < b$, et $f \in \mathcal{F}(I, \mathbb{R}^n)$. Pour $i \in \{1, \cdots, n\}$, on note f_i la i-ième composante de f. Ainsi, pour tout $t \in I$, on a $f(t) = (f_1(t), \cdots, f_n(t))$ (on remarquera que $f_i \in \mathcal{F}(I, \mathbb{R})$).

G1 Soit R un automorphisme orthogonal de $\mathbb{R}^n$. Montrer que si f est de longueur bornée sur $[a, b]$ alors $R \circ f$ l'est aussi sur $[a, b]$ et que :

$$L_a^b(R \circ f) = L_a^b(f).$$

G2 On suppose que f est de longueur bornée sur $[a, b]$. Montrer que pour tout $i \in \{1, \cdots, n\}$, la fonction f_i est de longueur bornée sur $[a, b]$ et que :

$$L_a^b(f_i) \leqslant L_a^b(f).$$

G3 On suppose que pour tout $i \in \{1, \cdots, n\}$, f_i est de longueur bornée sur $[a, b]$. Démontrer que f est de longueur bornée sur $[a, b]$ et que :

$$L_a^b(f) \leqslant \sum_{i=1}^{i=n} L_a^b(f_i).$$

G4 Démontrer que f est de longueur bornée sur tout segment de I si et seulement si pour tout $i \in \{1, \cdots, n\}$, f_i est à variations bornées.

G5 On suppose maintenant que f est de longueur bornée sur tout segment de I. Soient α, β, γ dans I. Établir l'égalité :

$$L_\alpha^\beta(f) + L_\beta^\gamma(f) = L_\alpha^\gamma(f).$$

Dans toute la suite, on suppose que $f \in \mathcal{F}(I, \mathbb{R}^n)$ est de classe C^1 sur I et on rappelle que :

$$\forall t \in I,\ f'(t) = (f_1'(t), \cdots, f_n'(t)).$$

Prouver que f est de longueur bornée sur tout segment de I.

G7 Soit T un endomorphisme de $\mathbb{R}^n$. Montrer que $T \circ f$ est de classe $\mathcal{C}^1$ sur I et que $(T \circ f)' = T \circ f'$.

G8 On définit la fonction w, pour $x \in I$, par $w(x) = L_a^x(f)$ et on considère $t \in I$.

G8a Montrer qu'il existe $\vec{u} \in \mathbb{R}^n$ tel que $\|\vec{u}\| = 1$ et $f'(t) = \|f'(t)\|\,\vec{u}$.

G8b Prouver qu'il existe R un automorphisme orthogonal de $\mathbb{R}^n$ tel que :

$$R(\vec{u}) = (1, 0, \cdots, 0).$$

On pose alors $g = R \circ f$ et $(g_1, \ldots, g_n) = g$.

G8c Montrer que g est de classe $\mathcal{C}^1$ sur I et établir que :

$$g_1'(t) = \left\|f'(t)\right\| \text{ et } \forall i \in \{2, \cdots, n\},\ g_i'(t) = 0.$$

G8d Montrer que g est de longueur bornée sur tout segment de I.

G8e Soit $v \in \mathbb{R}^*$ tel que $t + v \in I$, prouver que :

$$\frac{1}{v} L_t^{t+v}(g_1) \leqslant \frac{1}{v} L_t^{t+v}(f) \leqslant \frac{1}{v} \sum_{i=1}^{i=n} L_t^{t+v}(g_i).$$

G8f En déduire que w est dérivable en t et que $w'(t) = \|f'(t)\|$.

G9 Établir que :

$$L_a^b(f) = \int_a^b \left\|f'(t)\right\| dt.$$

G10 Soit $h \in \mathcal{F}([a,b], \mathbb{R}^n)$ une fonction de classe $\mathcal{C}^1$ sur $[a, b[$ telle que l'intégrale $\displaystyle\int_a^b h'(t)\, dt$ soit absolument convergente. On veut montrer que h est de longueur bornée sur $[a,b]$ et exprimer $L_a^b(h)$. On considère $\varepsilon \in \mathbb{R}_+^*$.

G10a Prouver que $h|_{[a,b[}$ admet une limite finie en b. On notera H cette limite.

G10b Soit $x \in [a, b]$. Montrer que :

$$\|h(x) - h(b)\| \leqslant \|H - h(b)\| + \int_x^b \left\|h'(t)\right\| dt.$$

G10c Soit σ une subdivision de $[a,b]$. Établir que :

$$\ell(\sigma,h) \leqslant \|H - h(b)\| + \int_a^b \left\|h'(t)\right\| \, dt.$$

G10d Montrer qu'il existe $d \in]a,b[$ tel que :

$$\|H - h(b)\| - \frac{\varepsilon}{2} \leqslant \|h(d) - h(b)\| - \int_d^b \left\|h'(t)\right\| \, dt.$$

G10e Montrer qu'il existe une subdivision σ' de $[a,d]$ telle que :

$$\int_a^d \left\|h'(t)\right\| \, dt - \frac{\varepsilon}{2} \leqslant \ell(\sigma', h).$$

G10f Montrer qu'il existe une subdivision, σ'' de $[a,b]$ telle que :

$$\|H - h(b)\| + \int_a^b \left\|h'(t)\right\| \, dt - \varepsilon \leqslant \ell(\sigma'', h).$$

G10g Conclure.

G11 Soit $h \in \mathcal{F}([a,b],\mathbb{R}^n)$ telle que h soit de classe $\mathcal{C}^1$ sur $[a,b[$ et que l'intégrale $\displaystyle\int_a^b h'(t)\,dt$ ne soit pas absolument convergente. Soit $A \in \mathbb{R}$.

G11a Démontrer qu'il existe $c \in [a,b[$ tel que $\displaystyle\int_a^c \|h'(t)\| \, dt > A + 1$.

G11b Montrer qu'il existe une subdivision σ de $[a,b]$ telle que $\ell(\sigma,h) > A$.

G11c Prouver que h n'est pas de longueur bornée sur $[a,b]$.

3.2 Corrigé

– A – Premières propriétés

On notera $\mathcal{VB}(I,\mathbb{R})$ l'ensemble des fonctions à variations bornées de I dans $\mathbb{R}$.

1. Si f est croissante [resp. décroissante], alors $g = f$ [resp. $g = 0$] est croissante, $h = 0$ [resp. $h = f$] est décroissante et $f = g + h \in \mathcal{VB}(I,\mathbb{R})$.
2.

(a) $\mathcal{VB}(I,\mathbb{R})$ est non vide puisqu'il contient les fonctions monotones (ou tout simplement la fonction nulle) et pour $f_1 = g_1+h_1$, $f_2 = g_2+h_2$ dans $\mathcal{VB}(I,\mathbb{R})$ avec g_1, g_2 croissantes, h_1, h_2 décroissante, λ dans $\mathbb{R}^+$ [resp. dans $\mathbb{R}^-$], la fonction $g = g_1 + \lambda g_2$ [resp. $g = g_1 + \lambda h_2$] est croissante, la fonction $h = h_1 + \lambda h_2$ [resp. $h = h_1 + \lambda g_2$] est décroissante et $f_1 + \lambda f_2 = g + h \in \mathcal{VB}(I,\mathbb{R})$.
On a ainsi montré que $\mathcal{VB}(I,\mathbb{R})$ est un sous-espace vectoriel de $\in \mathcal{F}(I,\mathbb{R})$.

(b) L'ensemble des foncions croissantes est contenu dans $\mathcal{VB}(I,\mathbb{R})$, donc $\mathcal{VB}(I,\mathbb{R})$ contient l'espace vectoriel engendré par ces fonctions croissantes et $f = g + h = g - (-h)$, où g est croissante, h décroissante, est combinaison linéaire de deux fonctions croissantes. D'où le résultat annoncé.

3. Soit $f = g+h \in \mathcal{VB}(I,\mathbb{R})$ où g est croissante, h décroissante et $\alpha \in I$. La fonction $k = g - g(\alpha)$ est croissante nulle en α, la fonction $\ell = h + g(\alpha)$ est décroissante et $f = k + \ell$.

4. Pour tout $x \in [a,b]$, on a $g(a) \leq g(x) \leq g(b)$, $h(b) \leq h(x) \leq h(a)$ et :

$$h(x) - h(a) \leq f(x) - f(a) = g(x) - g(a) + h(x) - h(a) \leq g(x) - g(a)$$

puisque $g(x) - g(a) \geq 0$ et $h(x) - h(a) \leq 0$. C'est vrai en particulier pour $x = b$.

5. Comme $h(b) \leq h(x)$ et $g(x) \leq g(b)$ pour tout $x \in [a,b]$, on déduit de ce qui précède que pour tout $x \in [a,b]$, on a :

$$h(b) - h(a) \leq f(x) - f(a) \leq g(b) - g(a)$$

soit :

$$h(b) - h(a) + f(a) = h(b) + g(a) \leq f(x) \leq f(a) + g(b) - g(a) = h(a) + g(b)$$

et f est bornée sur $[a,b]$.
Ou plus simplement, on peut dire que f est bornée sur $[a,b]$ comme somme de deux fonctions bornées.

6. Une fonction monotone admettant des limites à droite et gauche en tout point de $\overset{\circ}{I}$, il en est de même de $f \in \mathcal{VB}(I,\mathbb{R})$.
Rappelons la démonstration de la première affirmation.
Quitte à remplacer g par $-g$, on peut supposer g croissante.
Pour $x \in \overset{\circ}{I}$ et $a < x$ dans I, l'ensemble $A = \{g(t) \mid a < t < x\}$ est non vide majoré par $g(x)$, il admet donc une borne supérieure $\mu =$

$\sup_{a<t<x} g(t) \leq g(x)$. Par définition de la borne supérieure, pour tout réel $\varepsilon > 0$, il existe $x_0 \in]a, x[$ tel que $\mu - \varepsilon < g(x_0) \leq \mu$ et avec la croissance de g, on a :

$$\forall t \in]x_0, x[, \ \mu - \varepsilon < g(x_0) \leq g(t) \leq \mu.$$

On a donc ainsi montré que $\mu = \lim_{t \to x^-} g(t) = g(x^-)$.
On procède de même pour l'existence de la limite à droite $g(x^+)$.
Pour $x < y$ dans $\overset{\circ}{I}$ a, b dans I tels que $a < x < b$, on a :

$$g\left(x^+\right) = \inf_{x<t<b} g(t) = \inf_{x<t<y} g(t), \ g\left(y^-\right) = \sup_{a<t<y} g(t) = \sup_{x<t<y} g(t),$$

ce qui entraîne $g(x^+) \leq g(y^-)$.

– B – Fonctions de longueur bornée

On notera $\mathcal{LB}([a,b], \mathbb{R})$ l'ensemble des fonctions de longueur bornée sur $[a,b]$.

1. Pour toute subdivision σ de $[a,b]$, on a $\ell(\sigma, f) \geq 0$ et

$$L_a^b(f) = \sup_{\sigma} \ell(\sigma, f) \geq 0$$

si $a < b$.

2. $\sigma = (a,b)$ étant une subdivision de $[a,b]$, on a :

$$0 \leq \ell(\sigma, f) = |f(b) - f(a)| \leq L_a^b(f).$$

3. Pour toute subdivision σ de $[a,b]$, on a :

$$\begin{aligned}\ell(\sigma, f+g) &= \sum_{k=1}^{p} |f(\sigma_k) - f(\sigma_{k-1}) + g(\sigma_k) - g(\sigma_{k-1})| \\ &\leq \sum_{k=1}^{p} |f(\sigma_k) - f(\sigma_{k-1})| + \sum_{k=1}^{p} |g(\sigma_k) - g(\sigma_{k-1})| \\ &\leq L_a^b(f) + L_a^b(g)\end{aligned}$$

et en conséquence $L_a^b(f+g) \leq L_a^b(f) + L_a^b(g)$.

4.

(a) L'ensemble $\{j \in \{0, \cdots, p\} \mid \sigma_j < c\}$ [resp. $\{j \in \{0, \cdots, p\} \mid \sigma_j > c\}$] étant fini non vide dans $\mathbb{N}$ ($\sigma_0 = a < c$ et $\sigma_p = b > c$) il admet un plus petit élément $r \in \{1, \cdots, p\}$ et un plus grand élément $q \in \{0, \cdots, p-1\}$.
En fait, on a $r = q + 1$ puisque $\sigma_q < c < \sigma_{q+1}$ et σ est strictement croissante.

(b) La suite σ étant strictement croissante, on a par définition de q et r :

$$\sigma'_0 = \sigma_0 = a < \cdots < \sigma_q = \sigma'_q < c = \sigma'_{q+1}$$

et :

$$\sigma''_0 = c < \sigma_r = \sigma''_1 < \cdots < \sigma_p = \sigma''_{p-r+1} = b$$

ce qui signifie que σ' [resp. σ''] est une subdivision de $[a, c]$ [resp. $[c, b]$].

(c) On a :

$$\begin{aligned}
\ell(\sigma, f) &= \sum_{k=1}^{q} |f(\sigma_k) - f(\sigma_{k-1})| + \sum_{k=r}^{p} |f(\sigma_k) - f(\sigma_{k-1})| \\
&= \sum_{k=1}^{q} \left|f\left(\sigma'_k\right) - f\left(\sigma'_{k-1}\right)\right| + |f(\sigma_r) - f(\sigma_q)| \\
&\qquad + \sum_{k=r+1}^{p} |f(\sigma_k) - f(\sigma_{k-1})|
\end{aligned}$$

(si $q = 0$, par exemple pour $\sigma = (a, b)$, la première somme vaut 0 et la dernière somme vaut 0 si $r = p$), ce qui s'écrit :

$$\begin{aligned}
\ell(\sigma, f) = &\sum_{k=1}^{q} \left|f\left(\sigma'_k\right) - f\left(\sigma'_{k-1}\right)\right| + \left|f\left(\sigma''_1\right) - f\left(\sigma'_q\right)\right| \\
&+ \sum_{k=2}^{p-r+1} \left|f\left(\sigma''_k\right) - f\left(\sigma''_{k-1}\right)\right|
\end{aligned}$$

avec :

$$\begin{aligned}
\left|f\left(\sigma''_1\right) - f\left(\sigma'_q\right)\right| &\leq \left|f\left(\sigma'_q\right) - f(c)\right| + \left|f(c) - f\left(\sigma''_1\right)\right| \\
&\leq \left|f\left(\sigma'_q\right) - f\left(\sigma'_{q+1}\right)\right| + \left|f\left(\sigma''_0\right) - f\left(\sigma''_1\right)\right|
\end{aligned}$$

et donc :

$$\begin{aligned}
\ell(\sigma, f) &\leq \sum_{k=1}^{q+1} \left|f\left(\sigma'_k\right) - f\left(\sigma'_{k-1}\right)\right| + \sum_{k=1}^{p-r+1} \left|f\left(\sigma''_k\right) - f\left(\sigma''_{k-1}\right)\right| \\
&\leq \ell\left(\sigma', f\right) + \ell\left(\sigma'', f\right)
\end{aligned}$$

(d) Si f est de longueur bornée sur $[a,c]$ et $[c,b]$, on déduit de ce qui précède que pour tout subdivision σ de $[a,b]$, on a :

$$\ell(\sigma,f) \leq \ell\left(\sigma',f\right) + \ell\left(\sigma'',f\right) \leq L_a^c(f) + L_c^b(f)$$

et en conséquence, f est de longueur bornée sur $[a,b]$ avec :

$$L_a^b(f) \leq L_a^c(f) + L_c^b(f)$$

5.

(a) Si $\sigma' = (\sigma_0 = a < \sigma_1 < \cdots < \sigma_q = c)$ est une subdivision de $[a,c]$ et $\sigma'' = (\sigma_q = c < \sigma_{q+1} < \cdots < \sigma_p = b)$ est une subdivision de $[b,c]$, alors $\sigma = (\sigma_0 = a < \sigma_1 < \cdots < \sigma_q < \cdots < \sigma_p = b)$ est une subdivision de $[a,b]$ et on a :

$$\begin{aligned}\ell\big(\sigma',f\big) + \ell\big(\sigma'',f\big) &= \sum_{k=1}^{q} |f(\sigma_k) - f(\sigma_{k-1})| + \sum_{k=q+1}^{p} |f(\sigma_k) - f(\sigma_{k-1})| \\ &= \sum_{k=1}^{p} |f(\sigma_k) - f(\sigma_{k-1})| = \ell(\sigma,f)\end{aligned}$$

(b) De ce qui précède, on déduit que pour toute subdivision σ' de $[a,c]$ et toute subdivision σ'' de $[c,b]$, on a, si f est de longueur bornée sur $[a,b]$:

$$\ell\left(\sigma',f\right) \leq \ell\left(\sigma',f\right) + \ell\left(\sigma'',f\right) = \ell(\sigma,f) \leq L_a^b(f)$$

et :

$$\ell\left(\sigma'',f\right) \leq \ell\left(\sigma',f\right) + \ell\left(\sigma'',f\right) = \ell(\sigma,f) \leq L_a^b(f)$$

ce qui entraîne que f est de longueur bornée sur $[a,c]$ et $[c,b]$. Puis avec :

$$\ell\left(\sigma',f\right) \leq L_a^b(f) - \ell\left(\sigma'',f\right)$$

on déduit que $L_a^c(f) \leq L_a^b(f) - \ell(\sigma'',f)$ pour toute subdivision σ'' de $[c,b]$, donc $\ell(\sigma'',f) \leq L_a^b(f) - L_a^c(f)$ et $L_c^b(f) \leq L_a^b(f) - L_a^c(f)$, soit $L_a^b(f) \geq L_a^c(f) + L_c^b(f)$.

6. Si f est de longueur bornée sur tout segment de I, **B.4.d.** et **B.5.b.** nous disent que $L_\alpha^\gamma(f) = L_\alpha^\beta(f) + L_\beta^\gamma(f)$ pour $\alpha < \gamma < \beta$. Pour $\alpha = \gamma$ [resp. $\gamma = \beta$], on $L_\alpha^\gamma(f) = 0$ [resp. $L_\beta^\gamma(f) = 0$] et $L_\alpha^\beta(f) + L_\beta^\gamma(f) = L_\alpha^\beta(f) - L_\beta^\alpha(f) = 0$ [resp. $L_\alpha^\gamma(f) = L_\alpha^\beta(f) = L_\alpha^\beta(f) + L_\beta^\gamma(f)$]. L'égalité

est donc vraie pour $\alpha \leq \gamma \leq \beta$.
Si $\gamma \leq \alpha \leq \beta$, on a :

$$\begin{aligned} L_{\alpha}^{\beta}(f) + L_{\beta}^{\gamma}(f) &= L_{\alpha}^{\beta}(f) - L_{\gamma}^{\beta}(f) \\ &= L_{\alpha}^{\beta}(f) - \left(L_{\gamma}^{\alpha}(f) + L_{\alpha}^{\beta}(f)\right) \\ &= -L_{\gamma}^{\alpha}(f) = L_{\alpha}^{\gamma}(f) \end{aligned}$$

Et on procède de même pour les autres cas de figure.

– C – Longueur bornée et à variations bornées

1. On peut remarquer que pour toute fonction $f \in \mathcal{F}(I, \mathbb{R})$, tout réel λ et toute subdivision σ de $[a, b] \subset I$, on a $\ell(\sigma, \lambda f) = |\lambda| \ell(\sigma, f)$ et pour $f \in \mathcal{LB}([a, b], \mathbb{R})$, on a $\lambda f \in \mathcal{LB}([a, b], \mathbb{R})$ avec $L_a^b(\lambda f) = |\lambda| L_a^b(f)$. En particulier, $L_a^b(-f) = L_a^b(f)$

   (a) Pour q croissante et toute subdivision σ de $[a, b] \subset I$, on a :

   $$\begin{aligned} \ell(\sigma, q) &= \sum_{k=1}^{p} |q(\sigma_k) - q(\sigma_{k-1})| = \sum_{k=1}^{p} (q(\sigma_k) - q(\sigma_{k-1})) \\ &= q(\sigma_p) - q(\sigma_0) = q(b) - q(a) = |q(b) - q(a)| \end{aligned}$$

   et en conséquence, q est de longueur bornée avec

   $$L_a^b(q) = |q(b) - q(a)|.$$

   Si q est décroissante, $-q$ est croissante et $L_a^b(q) = L_a^b(-q) = |q(b) - q(a)|$.

   (b) De **B.3.** et **C.1.a.** on déduit qu'une fonction à variations bornées sur I est de longueur bornée sur tout segment de I.

2. Pour $t < t'$ dans I, on a, si f est de longueur bornée sur tout segment de I :

$$\begin{aligned} 2\left(g\left(t'\right) - g(t)\right) &= f\left(t'\right) - f(t) + L_{\lambda}^{t'}(f) - L_{\lambda}^{t}(f) \\ &= f\left(t'\right) - f(t) + L_{t}^{t'}(f) \\ &\geq f\left(t'\right) - f(t) + \left|f\left(t'\right) - f(t)\right| \geq 0 \end{aligned}$$

La fonction g est donc croissante sur I.
En écrivant que

$$h(t) = -\frac{1}{2}\left(-f(t) + L_\lambda^t(f)\right) = -\frac{1}{2}\left((-f)(t) + L_\lambda^t(-f)\right)$$

on déduit que h est décroissante sur I.
Il en résulte que $f = g + h$ est à variations bornées sur I.

3. Les deux questions qui précèdent nous disent qu'une fonction $f \in \mathcal{F}(I, \mathbb{R})$ est à variations bornées sur I si, et seulement si, elle est de longueur bornée sur tout segment de I.

Quelques résultats supplémentaires

- La définition de fonctions de longueur bornée s'étend aux fonctions à valeurs dans un espace métrique.
- Une fonction λ-lipschitzienne sur I (par exemple dérivable à dérivée bornée) est de longueur bornée sur tout segment de I avec $L_a^b(f) \leq \lambda(b-a)$.
- La fonction $t \mapsto L_a^t(f)$ est croissante sur $[a, b]$.
- Si f est continue à gauche [resp. à droite] en $c \in]a, b[$, il en est alors de même de $t \mapsto L_a^t(f)$.
- Comme une fonction monotone est dérivable presque partout, il est de même d'une fonction à variations bornées.
- Comme les fonctions monotones, les fonctions à variations bornées n'ont que des discontinuité de première espèce et l'ensemble de ces points de discontinuité est dénombrable.
- Pour f, g à variations bornées sur I, on a $L_a^b(fg) \leq \|g\|_\infty L_a^b(f) + \|f\|_\infty L_a^b(g)$.
- Si f est à variations bornées sur I minorée par $\lambda > 0$, alors $\frac{1}{f}$ est à variations bornées et $L_a^b\left(\frac{1}{f}\right) \leq \frac{1}{\lambda^2} L_a^b(f)$.
- La fonction $x \mapsto x^\alpha \sin\left(\frac{1}{x^\beta}\right)$ est à variations bornées sur $[0, 1]$ si, et seulement si, $\alpha > \beta$.

– D – Cas des fonctions de classe $\mathcal{C}^1$

1. Pour $u < v$ dans I et f de classe $\mathcal{C}^1$, on a :

$$|f(v) - f(u)| = \left|\int_u^v f'(t)\, dt\right| \leq \int_u^v \left|f'(t)\right| dt$$

2.

(a) Pour toute subdivision σ de $[a,b] \subset I$, on a :

$$\begin{aligned}\ell(\sigma, f) &= \sum_{k=1}^{p} |f(\sigma_k) - f(\sigma_{k-1})| \\ &\leq \sum_{k=1}^{p} \int_{\sigma_{k-1}}^{\sigma_k} |f'(t)|\, dt = \int_a^b |f'(t)|\, dt\end{aligned}$$

(b) Il en résulte que f est de longueur bornée sur $[a,b]$ avec $L_a^b(f) \leq \int_a^b |f'(t)|\, dt$.
La fonction f est donc à variations bornées d'après **C.3.** puisque $[a,b]$ est un quelconque intervalle de I (la question **D.5.** est curieuse).

3.

(a) La fonction f' qui est continue sur le compact $[a,b]$ y est uniformément continue et pour $\varepsilon > 0$ donné, on peut trouver un réel $\eta > 0$ tel que $|f'(x) - f'(y)| < \frac{\varepsilon}{b-a}$ pour tous x, y dans $[a,b]$ tels que $|x - y| < \eta$. Désignant par p un entier naturel non nul tel que $\frac{b-a}{p} < \eta$ et par σ la subdivision définie par $\sigma_k = a + k\frac{b-a}{p}$ pour k compris entre 0 et p, on aura pour tous x, y dans $[\sigma_{i-1}, \sigma_i]$, $|x - y| \leq \sigma_i - \sigma_{i-1} = \frac{b-a}{p} < \eta$ et $|f'(x) - f'(y)| < \frac{\varepsilon}{b-a}$.

(b) Le théorème des accroissements finis (faut-il le prouver ici ?) nous dit qu'il existe $c_i \in]\sigma_{i-1}, \sigma_i[$ tel que $f(\sigma_i) - f(\sigma_{i-1}) = f'(c_i)(\sigma_i - \sigma_{i-1})$.

(c) On a, pour $1 \leq i \leq p$:

$$\begin{aligned}\int_{\sigma_{i-1}}^{\sigma_i} |f'(t)|\, dt &\leq \int_{\sigma_{i-1}}^{\sigma_i} |f'(t) - f'(c_i)|\, dt + \int_{\sigma_{i-1}}^{\sigma_i} |f'(c_i)|\, dt \\ &\leq \frac{\varepsilon}{b-a}(\sigma_i - \sigma_{i-1}) + |f'(c_i)|(\sigma_i - \sigma_{i-1}) \\ &\leq \frac{\varepsilon}{b-a}(\sigma_i - \sigma_{i-1}) + |f(\sigma_i) - f(\sigma_{i-1})|\end{aligned}$$

soit :

$$|f(\sigma_i) - f(\sigma_{i-1})| \geq \int_{\sigma_{i-1}}^{\sigma_i} |f'(t)|\, dt - \frac{\varepsilon}{b-a}(\sigma_i - \sigma_{i-1}).$$

(d) Il en résulte que :

$$\begin{aligned}\ell(\sigma, f) &= \sum_{k=1}^{p} |f(\sigma_k) - f(\sigma_{k-1})| \\ &\geq \sum_{k=1}^{p} \int_{\sigma_{i-1}}^{\sigma_i} |f'(t)|\, dt - \frac{\varepsilon}{b-a} \sum_{k=1}^{p} (\sigma_i - \sigma_{i-1}) \\ &\geq \int_a^b |f'(t)|\, dt - \varepsilon.\end{aligned}$$

4. Il en résulte que $L_a^b(f) \geq \ell(\sigma, f) \geq \int_a^b |f'(t)|\, dt - \varepsilon$. Comme $\varepsilon > 0$ est quelconque, cela équivaut à $L_a^b(f) \geq \int_a^b |f'(t)|\, dt$. Avec **D.2.b.** on conclut à l'égalité $L_a^b(f) = \int_a^b |f'(t)|\, dt$.
5. C'est fait en **D.2.b.**

– E – Cas des fonctions périodiques

1. Par définition de la partie entière, on a $p(x) \leq \frac{x}{T} < p(x) + 1$, ce qui équivaut à $0 \leq x - p(x)T < T$.
2. La fonction p est croissante à valeurs entières, donc $p(a) \leq p(b)$ dans $\mathbb{Z}$ si $a \leq b$, ce qui équivaut à $p(a) = p(b)$ ou $p(a) \leq p(b) - 1$.
3.
   (a) Comme T et $x - p(x)T$ sont dans $[0, T]$ et p, f sont définies sur $\mathbb{R}$, les fonctions g et h sont bien définies sur $\mathbb{R}$.

   (b) De $0 \leq x - p(x)T < T$, k croissante sur $[0, T]$ avec $k(0) = 0$, on déduit que :

$$0 = k(0) \leq k(x - p(x)T) \leq k(T)$$

   et :

$$p(x)k(T) \leq g(x) \leq (p(x) + 1)k(T)$$

   Si $a \leq b$, on a soit $p(a) = p(b)$ et dans ce cas :

$$g(b) - g(a) = k(b - p(b)T) - k(a - p(b)T) \geq 0$$

   soit $p(a) + 1 \leq p(b)$ et dans ce cas :

$$g(a) \leq (p(a) + 1)k(T) \leq p(b)k(T) \leq g(b).$$

   La fonction g est donc croissante sur $\mathbb{R}$.

(c) On a :

$$\begin{aligned}h(x) = f(x) - g(x) &= f(x) - p(x)\,k(T) - k(x - p(x)\,T)\\ &= f(x) - p(x)\,k(T) + \ell(x - p(x)\,T) - f(x - p(x)\,T)\\ &= -p(x)\,k(T) + \ell(x - p(x)\,T)\end{aligned}$$

puisque f est T-périodique et $p(x)$ entier.

(d) Comme ℓ est décroissante sur $[0,T]$ et f est T-périodique, on a pour tout $u \in [0,T]$:

$$\ell(0) \geq \ell(u) \geq \ell(T) = f(T) - k(T) = f(0) - k(T)$$

(e) Ayant vu en **E.3.b.** que g est croissante, il reste à vérifier que h est décroissante pour montrer que f est à variations bornées.
Pour $a < b$, on a soit $p(a) = p(b)$ et dans ce cas :

$$\begin{aligned}h(b) - h(a) &= \ell(b - p(b)\,T) - \ell(a - p(a)\,T) + (p(a) - p(b))\,k(T)\\ &= \ell(b - p(b)\,T) - \ell(a - p(b)\,T) \leq 0\end{aligned}$$

puisque ℓ est décroissante, soit $1 + p(a) \leq p(b)$ et dans ce cas :

$$\begin{aligned}h(b) - h(a) &= \ell(b - p(b)\,T) - \ell(a - p(a)\,T) + (p(a) - p(b))\,k(T)\\ &\leq \ell(0) - f(0) + k(T) + (p(a) - p(b))\,k(T)\\ &= -k(0) + (1 + p(a) - p(b))\,k(T)\\ &= (1 + p(a) - p(b))\,k(T) \leq 0\end{aligned}$$

en tenant compte de $\ell(b - p(b)\,T) \leq \ell(0)$, $\ell(a - p(a)\,T) \geq f(0) - k(T)$, $k(0) = 0$ et $k(T) \geq k(0) = 0$. La fonction h est donc décroissante.

4.

(a) Pour $x \in \mathbb{R}$, on a $[x] \leq x < [x] + 1$ et en particulier $-1 \leq x - [x] - 1 < 0$. La fonction ψ est donc bien définie sur $\mathbb{R}$ et à valeurs dans $]-\infty, -1]$.
Avec $[x+1] = [x] + 1$, on déduit que $\psi(x+1) = \psi(x)$ et ψ est 1-périodique.

(b) La fonction $\psi_{|[0,1[} : x \mapsto \dfrac{1}{x-1}$ est décroissante sur $[0,1[$, donc à variations bornées sur cet intervalle.
La fonction ψ n'est pas à variations bornées sur $[0,1]$ puisque non bornée sur cet intervalle ($\lim\limits_{x\to 1^-} \psi(x) = \lim\limits_{x\to 1^-} \dfrac{1}{x-1} = -\infty$), donc ψ n'est pas à variations bornées sur $\mathbb{R}$.

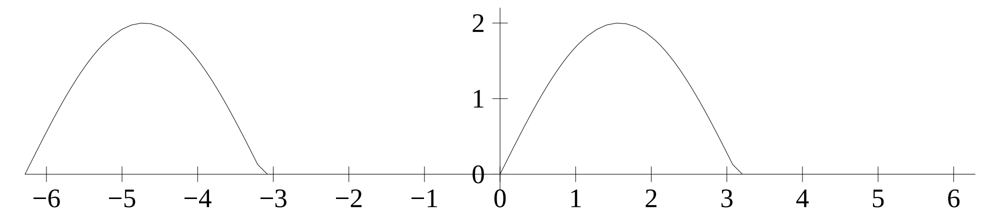



FIG. 3.1 – $y = |\sin(x)| + \sin(x)$

5. Voir la figure 3.1.
6. La fonction φ étant 2π-périodique sur $\mathbb{R}$, il suffit de montrer que $\varphi_{|[0,2\pi]}$ est à variations bornées pour déduire que φ à variations bornées sur $\mathbb{R}$. Comme φ est $\mathcal{C}^1$ sur $[0,\pi]$ et $[\pi, 2\pi]$, elle est de longueur bornée sur ces intervalles, donc de longueur bornée et à variations bornées.
7.
   (a) Pour $n \in \mathbb{N}$, on a d'après **A.4.** :
   $$g\left(2n\pi + \frac{\pi}{2}\right) - g(2n\pi) \geq f\left(2n\pi + \frac{\pi}{2}\right) - f(2n\pi) = f\left(\frac{\pi}{2}\right) - f(0) = 2.$$
   (b) On procède par récurrence sur $n \geq 0$. Pour $n = 0$, c'est clair ($g(0) = 0$). Supposant le résultat acquis jusqu'au rang $n \geq 0$, on a pour $n = 2p$:
   $$\begin{aligned} g((n+1)\pi) &= g(2p\pi + \pi) \geq g\left(2p\pi + \frac{\pi}{2}\right) \\ &\geq g(2p\pi) + 2 \geq 2p + 2 = n + 2 > n + 1 \end{aligned}$$
   (la fonction g est croissante) et pour $n = 2p + 1$:
   $$\begin{aligned} g((n+1)\pi) &= g(2p\pi + 2\pi) \geq g\left(2p\pi + \frac{\pi}{2}\right) \\ &\geq g(2p\pi) + 2 \geq 2p + 2 = n + 1 \end{aligned}$$
   On a donc $g(n\pi) \geq n$ pour tout $n \in \mathbb{N}$.
   (c) Comme g est croissante, on déduit de la question précédente que $\lim\limits_{x \to +\infty} g(x) = +\infty$.
   (d) Avec $h(x) = f(x) - g(x)$ et f bornée, on déduit que $\lim\limits_{x \to +\infty} h(x) = -\infty$.

– F – Une fonction dérivable bornée non à variations bornées

1.
   (a) La fonction f est paire.

   (b) La fonction f est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^*$ avec $f'(x) = 2x \sin\left(\frac{1}{x^2}\right) - \frac{2}{x}\cos\left(\frac{1}{x^2}\right)$.
   De $\left|\frac{f(x) - f(0)}{x}\right| = |x| \left|\sin\left(\frac{1}{x^2}\right)\right| \leq |x|$ sur $\mathbb{R}^*$, on déduit que $\lim\limits_{x \to 0} \frac{f(x) - f(0)}{x} = 0$, ce qui signifie que f est dérivable en 0 avec $f'(0) = 0$.

   (c) Avec $f'\left(\frac{1}{\sqrt{2n\pi}}\right) = -2\sqrt{2n\pi} \underset{n \to +\infty}{\to} -\infty$, on déduit que f' n'est pas continue en 0. Donc f n'est pas de classe $\mathcal{C}^1$ sur $\mathbb{R}$.

   (d) Avec $\sin(t) \underset{t \to 0}{\sim} t$, on déduit que $f(x) \underset{x \to +\infty}{\sim} 1$ et $\lim\limits_{x \to +\infty} f(x) = 1$.

   (e) On en déduit que f est bornée sur $\mathbb{R}$.
   En fait avec $|\sin(t)| \leq |t|$, on déduit immédiatement que $|f(x)| \leq 1$ pour tout $x \in \mathbb{R}$.

2. Avec :
$$0 < \ln\left(1 + \frac{2}{4n-1}\right) \underset{n \to +\infty}{\sim} \frac{1}{2n},$$
on déduit que la série $\sum \ln\left(1 + \frac{2}{4n-1}\right)$ diverge.

3.
   (a) C'est évident.

b. et c. Le changement variable $x = \frac{1}{t^2}$, $dx = -\frac{2dt}{t^3} = -2x\sqrt{x}dt$ donne :
$$\int_{u_{n+1}}^{u_n} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt = \int_{-\frac{\pi}{2}+n\pi}^{\frac{\pi}{2}+n\pi} \frac{|\cos(x)|}{2x} dx$$
puis $x = n\pi + u$ donne :
$$\begin{aligned}\int_{u_{n+1}}^{u_n} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt &= \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} \frac{|\cos(u)|}{2(u+n\pi)} du \\ &\geq \frac{1}{2(n+1)\pi} \int_{-\frac{\pi}{2}}^{\frac{\pi}{2}} |\cos(u)|\, dx\end{aligned}$$

La divergence de $\sum \int_{u_{n+1}}^{u_n} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt$ en résulte alors.

d. Comme la suite $(u_n)_{n\geq 1}$ tend vers 0 en décroissant, la convergence de l'intégrale $\int_0^{u_1} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt$ entraînerait celle de la suite $(S_n)_{n\geq 1}$ définie par :

$$S_n = \int_{u_n}^{u_1} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt = \sum_{k=1}^{n-1} \int_{u_{k+1}}^{u_k} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt$$

ce qui contredit le résultat de la question précédente.

4.

(a) Avec $\left|x\sin\left(\frac{1}{x^2}\right)\right| \leq |x|$ pour $x \neq 0$, on déduit que l'intégrale $\int_0^1 x\sin\left(\frac{1}{x^2}\right) dx$ est absolument convergente.
Une intégration par parties donne pour $0 < \varepsilon < 1$:

$$\begin{aligned}\int_\varepsilon^1 \frac{1}{x}\cos\left(\frac{1}{x^2}\right) dx &= \int_\varepsilon^1 \frac{x^2}{x^3}\cos\left(\frac{1}{x^2}\right) dx \\ &= \left[-\frac{x^2}{2}\sin\left(\frac{1}{x^2}\right)\right]_\varepsilon^1 + \int_\varepsilon^1 x\sin\left(\frac{1}{x^2}\right) dx\end{aligned}$$

avec $\left|x\sin\left(\frac{1}{x^2}\right)\right| \leq |x|$ et $\left|x^2\sin\left(\frac{1}{x^2}\right)\right| \leq x^2$, ce qui entraîne la convergence de l'intégrale $\int_0^1 \frac{1}{x}\cos\left(\frac{1}{x^2}\right) dx$ et celle de $\int_0^1 f'(x)\,dx$.
Avec $\frac{2}{x}\cos\left(\frac{1}{x^2}\right) = 2x\sin\left(\frac{1}{x^2}\right) - f'(x)$, la divergence de l'intégrale $\int_0^{u_1} \frac{1}{t}\left|\cos\left(\frac{1}{t^2}\right)\right| dt$ et la convergence absolue de $\int_0^1 x\sin\left(\frac{1}{x^2}\right) dx$, on déduit que $\int_0^1 |f'(x)|\,dx$ diverge.

(b) La question précédente nous dit que $\lim_{x\to 0^+} \int_0^1 |f'(x)|\,dx = +\infty$ (divergence de l'intégrale d'une fonction positive).

5. Si $a < b$ et $ab \leq 0$, on a $a < 0 \leq b$ ou $a = 0 < b$, donc si f est de longueur bornée sur $[a,b]$, elle le sera sur $[a,0]$ dans le premier cas ou sur $[0,b]$ dans le second cas.

Dans le premier cas, comme f est $\mathcal{C}^1$ sur $[a, -\varepsilon]$ pour $\varepsilon > 0$ petit, on aura $\int_a^{-\varepsilon} |f'(x)|\, dx = L_a^{-\varepsilon}(f)$ et comme f' est impaire, cela équivaut à $L_a^{-\varepsilon}(f) = \int_\varepsilon^{-a} |f'(x)|\, dx$. Mais alors :

$$L_a^0(f) \geq L_a^{-\varepsilon}(f) = \int_\varepsilon^{-a} \left|f'(x)\right| dx \underset{\varepsilon \to 0}{\to} +\infty,$$

ce qui est impossible.
Pour le deuxième cas de figure, on procède de manière analogue.
La fonction f ne peut donc être de longueur bornée sur $[a, b]$.

6. Si $0 \notin J$, la fonction f est $\mathcal{C}^1$ sur J, donc à variation bornée.
Si $0 \in J$, J contient un intervalle de la forme $[a, 0]$ avec $a < 0$ ou $[0, b]$ avec $b > 0$ et n'est pas de longueur bornée sur cet intervalle, elle n'est donc pas à variations bornées sur J.

– G – Cas des fonctions à valeurs dans $\mathbb{R}^n$

1. Si R est orthogonal, il conserve la norme et pour toute subdivision σ de $[a, b]$, on a :

$$\begin{aligned}
\ell(\sigma, R \circ f) &= \sum_{k=1}^{p} \|R \circ f(\sigma_k) - R \circ f(\sigma_{k-1})\| \\
&= \sum_{k=1}^{p} \|R(f(\sigma_k) - f(\sigma_{k-1}))\| \\
&= \sum_{k=1}^{p} \|f(\sigma_k) - f(\sigma_{k-1})\| = \ell(\sigma, f)
\end{aligned}$$

Il en résulte que $R \circ f$ est de longueur bornée sur $[a, b]$ avec $L_a^b(R \circ f) = L_a^b(f)$.

2. Avec $|x_i| \leq \|x\|$ pour tout vecteur $x \in \mathbb{R}^n$ et tout indice i compris entre 1 et n, on déduit que $\ell(\sigma, f_i) \leq \ell(\sigma, f)$ pour toute subdivision σ de $[a, b]$ et $L_a^b(f_i) \leq L_a^b(f)$.

3. Avec $\|x\| \leq \|x\|_1 = \sum_{k=1}^{n} |x_k|$ pour tout vecteur $x \in \mathbb{R}^n$ (équivalence des normes sur $\mathbb{R}^n$), on déduit que $\ell(\sigma, f) \leq \sum_{k=1}^{n} \ell(\sigma, f_k)$ et f est de longueur bornée sur $[a, b]$.

4. Conséquence immédiate des deux questions précédentes compte tenu de l'équivalence entre variations bornées sur I et de longueur bornée sur tout segment de I.
5. C'est la même démonstration qu'en **B.4. B5.** et **B.6.**
6. Si f est $\mathcal{C}^1$ sur I, il en de même de toutes les fonctions à valeurs réelles et ces fonctions sont à variations bornées, donc de longueur bornée sur tout segment de I et il en est de même de f.
7. On sait qu'un endomorphisme T de $\mathbb{R}^n$ est de classe $\mathcal{C}^1$ sur $\mathbb{R}^n$ avec $dT(x) = T$ pour tout $x \in \mathbb{R}^n$. Il en résulte que $T \circ f$ est $\mathcal{C}^1$ sur I avec $d(T \circ f)(t) = dT(f(t)) \circ df(t)$, ce qui équivaut à dire que $(T \circ f)'(t) = T \circ f'(t)$ puisque $T \circ f$ et f sont à valeurs réelles.
8. On se fixe t dans I.
   (a) Pour $t \in I$ tel que $f'(t) \neq 0$, on pose $u_t = \dfrac{1}{\|f'(t)\|} f'(t)$ et pour t tel que $f'(t) = 0$, on pose $u_t = e_1$ où $\mathcal{B} = (e_i)_{1 \leq i \leq n}$ est la base canonique de $\mathbb{R}^n$.
   (b) Le vecteur u_t peut se prolonger en une base orthonormée $\mathcal{B}'$ de $\mathbb{R}^n$ et il existe un automorphisme orthogonal R_t qui transforme $\mathcal{B}'$ en $\mathcal{B}$. En particulier, on a $R_t(u_t) = e_1$.
   (c) La fonction $g_t = R_t \circ f$ est de classe $\mathcal{C}^1$ sur I avec $(g_t)'(x) = R_t(f'(x))$pour tout $x \in I$. On a en particulier :

$$(g_t)'(t) = R_t\left(f'(t)\right) = \left\|f'(t)\right\| R_t(u_t) = \left\|f'(t)\right\| e_1$$

   et en notant $g_t = (g_i)_{1 \leq i \leq n}$, cela signifie que $g_1'(t) = \|f'(t)\|$ et $g_i'(t) = 0$ pour i compris entre 2 et n.
   (d) Comme f est de longueur bornée sur tout segment de I, il en est de même de $g_t = R_t \circ f$ (on peut aussi dire que g_t est de classe $\mathcal{C}^1$ donc de longueur bornée sur tout segment de I).
   (e) Pour $v > 0$, on a :

$$L_t^{t+v}(g_1) \leq L_t^{t+v}(g) \leq \sum_{k=1}^{n} L_t^{t+v}(g_k)$$

   avec $L_t^{t+v}(g) = L_t^{t+v}(f)$ et en conséquence :

$$\frac{1}{v} L_t^{t+v}(g_1) \leq \frac{1}{v} L_t^{t+v}(f) \leq \frac{1}{v} \sum_{k=1}^{n} L_t^{t+v}(g_k)$$

Le résultat pour $v < 0$ se déduit de $L_t^{t+v}(h) = -L_{t+v}^t(g_1)$ pour tout fonction h de longueur bornée sur tout segment de I. En effet l'encadrement :

$$L_{t+v}^t(g_1) \leq L_{t+v}^t(g) \leq \sum_{k=1}^n L_{t+v}^t(g_k)$$

s'écrit :

$$-L_t^{t+v}(g_1) \geq -L_t^{t+v}(g) \geq -\sum_{k=1}^n L_t^{t+v}(g_k)$$

et divisant par $v < 0$, on a l'encadrement annoncé.

(f) En **D.** on a vu que $L_a^b(h) = \int_a^b |h'(t)|\, dt$ pour tout fonction h de classe $\mathcal{C}^1$ sur I et tous a, b dans I. L'encadrement se traduit donc par :

$$\frac{1}{v}\int_t^{t+v} \left|g_1'(t)\right| dt \leq \frac{1}{v}L_t^{t+v}(f) \leq \frac{1}{v}\sum_{k=1}^n \int_t^{t+v} \left|g_k'(t)\right| dt$$

avec :

$$\begin{aligned}\lim_{v\to 0}\frac{1}{v}\int_t^{t+v} \left|g_k'(t)\right| dt &= \lim_{v\to 0}\frac{1}{v}\left(\int_a^{t+v} \left|g_k'(t)\right| dt - \int_a^t \left|g_k'(t)\right| dt\right)\\ &= \left|g_k'(t)\right| = \begin{cases} \|f'(t)\| \text{ si } k = 1 \\ 0 \text{ si } 2 \leq k \leq n\end{cases}\end{aligned}$$

($x \mapsto \displaystyle\int_a^x h(t)\, dt$ est dérivable de dérivée h) et $L_t^{t+v}(f) = w(t+v) - w(t)$. On a donc :

$$\lim_{v\to 0}\frac{w(t+v) - w(t)}{v} = \left\|f'(t)\right\|$$

ce qui signifie que w est dérivable en t de dérivée $\|f'(t)\|$.

9. Comme $t \mapsto \|f'(t)\|$ est continue sur I, on déduit de ce qui précède que pour tout $t \in I$, on a :

$$w(t) = \int_a^t w'(x)\, dx + w(a) = \int_a^t w'(x)\, dx$$

soit :

$$\forall t \in I,\ L_a^t(f) = \int_a^t \left\|f'(x)\right\| dx$$

10.

(a) Comme h est de classe $\mathcal{C}^1$ sur $[a,b[$, on a pour tout $x \in [a,b[$:

$$h(x) = \int_a^x h'(t)\,dt + h(a) \underset{x\to b}{\to} \int_a^b h'(t)\,dt + h(a) = H$$

puisque l'intégrale de h' sur $[a,b[$ est convergente.

(b) Comme l'intégrale de h' sur $[a,b[$ est absolument convergente, on a pour tout $x \in [a,b[$:

$$\begin{aligned} \|h(b) - h(x)\| &\leq \|h(b) - H\| + \|H - h(x)\| \\ &\leq \|h(b) - H\| + \left\|\int_x^b h'(t)\,dt\right\| \\ &\leq \|h(b) - H\| + \int_x^b \left\|h'(t)\right\|dt \end{aligned}$$

Pour $x = b$, l'inégalité est triviale.

(c) Pour tout subdivision $\sigma = (\sigma_k)_{0\leq k\leq p}$ de $[a,b]$ $(p \geq 2)$, on a :

$$\begin{aligned} \ell(\sigma,h) &= \sum_{k=1}^{p} \|h(\sigma_k) - h(\sigma_{k-1})\| \\ &\leq \sum_{k=1}^{p-1} \|h(\sigma_k) - h(\sigma_{k-1})\| + \|h(b) - h(\sigma_{p-1})\| \\ &\leq \sum_{k=1}^{p-1} \left\|\int_{\sigma_{k-1}}^{\sigma_k} h'(t)\,dt\right\| + \|h(b) - H\| + \int_{\sigma_{p-1}}^{b} \left\|h'(t)\right\|dt \\ &\leq \|h(b) - H\| + \sum_{k=1}^{p} \int_{\sigma_{k-1}}^{\sigma_k} \left\|h'(t)\right\|dt \end{aligned}$$

soit :

$$\ell(\sigma,h) \leq \|h(b) - H\| + \int_a^b \left\|h'(t)\right\|dt$$

Pour $p = 1$ c'est l'inégalité précédente avec $x = a$.

(d) On a :

$$\|h(b) - H\| = \lim_{x\to b^-} \|h(b) - h(x)\|$$

et :

$$\lim_{x\to b^-} \int_x^b \left\|h'(t)\right\|dt = 0$$

donc pour $\varepsilon' > 0$, il existe $d \in \left]a, b\right[$ tel que :

$$\forall x \in \left[d, b\right[, \ -\varepsilon' \leq \|h(b) - H\| - \|h(b) - h(x)\| \leq \varepsilon'$$

et :

$$\forall x \in \left[d, b\right[, \ 0 \leq \int_x^b \left\|h'(t)\right\| dt \leq \varepsilon'$$

On a donc, pour tout $x \in \left[d, b\right[$:

$$-\varepsilon' \leq \|h(b) - H\| - \|h(b) - h(x)\| + \int_x^b \left\|h'(t)\right\| dt \leq 2\varepsilon'$$

et en conséquence :

$$\|h(b) - H\| - 2\varepsilon' \leq \|h(b) - h(x)\| - \int_x^b \left\|h'(t)\right\| dt.$$

Prenant $\varepsilon' = \dfrac{\varepsilon}{4}$ et $x = d$, on a le résultat annoncé.

(e) Comme h est de classe $\mathcal{C}^1$ sur $\left[a, b\right[$, elle est de longueur bornée sur $[a, d]$ et :

$$\int_a^d \left\|h'(x)\right\| dx = L_a^d(h) = \sup_{\sigma \text{ subdivision de } [a,d]} \ell(\sigma, h)$$

et il existe une subdivision σ' de $[a, d]$ telle que :

$$\int_a^d \left\|h'(x)\right\| dx - \frac{\varepsilon}{2} \leq \ell\left(\sigma', h\right) \leq \int_a^d \left\|h'(x)\right\| dx.$$

(f) Si σ'' est la subdivision de $[a, b]$ obtenu en ajoutant à σ' le point b, on a alors :

$$\ell\left(\sigma'', h\right) = \ell\left(\sigma', h\right) + \|h(b) - h(d)\|$$

avec :

$$\|h(b) - h(d)\| \geq \|h(b) - H\| - \frac{\varepsilon}{2} + \int_d^b \left\|h'(t)\right\| dt$$

(question **G.10.d.**) et :

$$\ell\left(\sigma', h\right) \geq \int_a^d \left\|h'(x)\right\| dx - \frac{\varepsilon}{2}$$

ce qui donne :

$$\ell\left(\sigma'', h\right) \geq \|h(b) - H\| - \varepsilon + \int_a^b \left\|h'(t)\right\| dt.$$

(g) La question **G.10.c.** nous dit que h est de longueur bornée sur $[a,b]$ et que $L = \|h(b) - H\| + \int_a^b \|h'(t)\| \, dt$ est un majorant de $L_a^b(h)$ et la question précédente nous dit que pour tout $\varepsilon > 0$ on peut trouver une subdivision σ'' de $[a,b]$ telle que $L - \varepsilon \leq \ell(\sigma'', h)$. Cette quantité L est donc la borne supérieure des $\ell(\sigma, h)$ où σ décrit toutes les subdivisions de $[a,b]$. On a donc :

$$L_a^b(h) = \|h(b) - H\| + \int_a^b \left\|h'(t)\right\| dt.$$

11.

(a) Si l'intégrale de h' sur $[a,b[$ n'est pas absolument convergente, on a $\lim\limits_{x \to b} \displaystyle\int_a^x \|h'(t)\| \, dt = +\infty$ et pour tout réel $A > 0$, il existe $c \in [a,b[$ tel que $\displaystyle\int_a^c \|h'(t)\| \, dt > A + 1$.

(b) La fonction h étant de classe $\mathcal{C}^1$ sur $[a,c]$, elle est de longueur bornée sur $[a,c]$ avec $L_a^c(h) = \int_a^c \|h'(t)\| \, dt$ et par définition de la borne supérieure, on peut trouver une subdivision σ de $[a,c]$ telle $\ell(\sigma, h) > L_a^c(h) - 1 > A$.

(c) La question précédente nous dit que $\sup\limits_{\sigma \text{ subdivision de } [a,b]} \ell(\sigma, h) = +\infty$ et h n'est pas de longueur bornée sur $[a,b]$.

Chapitre 4

Agrégation interne 2008, épreuve 2

4.1 Énoncé

Introduction et notations

Dans ce problème, on note $\mathbb{N}$ l'ensemble des nombres entiers, $\mathbb{R}$ le corps des nombres réels.
On dit qu'un endomorphisme T d'un espace vectoriel est nilpotent s'il existe un nombre entier $s \geq 0$ tel que $T^s = 0$.
Si f est une fonction de classe $\mathcal{C}^\infty$ de la variable réelle x et n un entier ≥ 0, on note $f^{(n)}$ ou $\dfrac{d^n f}{dx^n}$ la dérivée n-ème de la fonction f.
Si g est une fonction de classe $\mathcal{C}^\infty$ de la variable réelle $x = (x_1, \cdots, x_n)$ définie dans une partie ouverte de $\mathbb{R}^n$, on note $\dfrac{\partial g}{\partial x_i}$ la dérivée partielle de g par rapport à la variable x_i, pour $1 \leq i \leq n$.
Pour des entiers p et n tels que $0 \leq p \leq n$, on définit les coefficients binomiaux par :

$$\binom{n}{p} = \frac{n!}{p!\,(n-p)!} = \frac{n\,(n-1)\cdots(n-p+1)}{p!} \text{ pour } 0 < p < n$$

et $\dbinom{n}{0} = \dbinom{n}{n} = 1$.
L'un des objets de ce problème est la démonstration de la formule de réversion de Lagrange qui permet de calculer, dans certains cas, la dérivée n-ème d'une fonction réciproque.

On étudie d'abord la suite $(u_n)_{n\geq 1}$ dont le terme général est l'unique solution ≥ 0 de l'équation :

$$x^n + x^{n-1} + \cdots + x - 1 = 0. \qquad (E_n)$$

Dans un premier temps, on établit directement une expression explicite de u_n comme somme d'une série convergente (parties **I** et **II**).
On établit ensuite la formule de réversion de Lagrange (partie **III**).
On applique enfin cette formule pour obtenir une autre démonstration de l'expression de u_n (partie **IV**).
On rappelle les résultats suivants qui pourront être utilisés sans démonstration :

A Lorsque l'entier n tend vers $+\infty$, on a l'équivalence (formule de Stirling) :

$$n! \underset{n\to+\infty}{\sim} n^n e^{-n}\sqrt{2\pi n}.$$

B Pour tout entier $q \geq 1$, la série entière :

$$\sum_{n\geq 0} (-1)^n \binom{n+q-1}{n} x^n$$

a un rayon de convergence égal à 1 et, pour $-1 < x < 1$, sa somme est égale à $\dfrac{1}{(1+x)^q}$.

C Le théorème des fonctions implicites pour une fonction F de classe $\mathcal{C}^\infty$, définie sur $\mathbb{R}^3$, peut s'énoncer ainsi :
on suppose qu'en un point (x_0, y_0, z_0) de $\mathbb{R}^3$, on a :

$$F(x_0, y_0, z_0) = 0 \text{ et } \frac{\partial F}{\partial x}(x_0, y_0, z_0) \neq 0$$

il existe alors un voisinage ouvert U de (x_0, y_0) dans $\mathbb{R}^2$, un voisinage ouvert V de z_0 dans $\mathbb{R}$ et une fonction $\varphi : U \to V$ caractérisée par la condition :

$$\forall (x,y) \in U,\ \forall z \in V,\ (F(x,y,z) = 0 \Leftrightarrow z = \varphi(x,y)).$$

La fonction φ est de classe $\mathcal{C}^\infty$ sur U et pour tout point (a,b) de U, on a :

$$F(a, b, \varphi(a,b)) = 0$$

ainsi que les relations :

$$\frac{\partial \varphi}{\partial x}(a,b) = -\frac{\frac{\partial F}{\partial x}(a,b,\varphi(a,b))}{\frac{\partial F}{\partial z}(a,b,\varphi(a,b))},\ \frac{\partial \varphi}{\partial y}(a,b) = -\frac{\frac{\partial F}{\partial y}(a,b,\varphi(a,b))}{\frac{\partial F}{\partial z}(a,b,\varphi(a,b))}$$

On dit que la fonction φ est définie implicitement sur U par la relation $F(x,y,z) = 0$.

D Soit $(a_{n,k})_{(n,k)\in\mathbb{N}^2}$ une suite double de nombres réels.

Si la somme $\sum_{n=0}^{+\infty}\left(\sum_{k=0}^{+\infty}|a_{n,k}|\right)$ est finie, alors les trois expressions :

$$\sum_{n=0}^{+\infty}\left(\sum_{k=0}^{+\infty}a_{n,k}\right),\ \sum_{k=0}^{+\infty}\left(\sum_{n=0}^{+\infty}a_{n,k}\right),\ \sum_{q=0}^{+\infty}\left(\sum_{n+k=q}^{+\infty}a_{n,k}\right)$$

ont un sens et sont égales. Leur valeur commune est notée $\sum_{n=0}^{+\infty}\sum_{k=0}^{+\infty}a_{n,k}$.

E Soit R un nombre réel >0. Si les fonctions f et g sont sommes de séries entières convergentes dans l'intervalle $]-R,R[$, leur somme $f+g$ et leur produit fg sont aussi sommes de séries entières convergentes dans le même intervalle.

– I – La suite (u_n)

1. Démontrer, pour tout entier $n\geq 1$, l'existence d'une unique solution réelle ≥ 0 de l'équation :

$$x^n+x^{n-1}+\cdots+x-1=0 \tag{4.1}$$

   Cette solution est notée u_n. Démontrer que l'on a $0\leq u_n\leq 1$.

2. Démontrer que la suite $(u_n)_{n\geq 1}$ est strictement décroissante.
3. Démontrer que pour tout $n\geq 1$, on a :

$$u_n^{n+1}-2u_n+1=0.$$

4.

   (a) Calculer u_2.

   (b) Démontrer que la suite $(u_n)_{n\geq 1}$ converge vers $\frac{1}{2}$.

5. Pour $n\geq 1$, on pose $\varepsilon_n=u_n-\frac{1}{2}$. Démontrer que $n\varepsilon_n$ tend vers 0 lorsque n tend vers $+\infty$.
6. En déduire, à l'aide de la question **I.3.** le développement asymptotique suivant de u_n, pour n tendant vers $+\infty$:

$$u_n=\frac{1}{2}+\frac{1}{4\cdot 2^n}+o\left(\frac{1}{2^n}\right)$$

7.

(a) Déterminer le plus petit entier $s \geq 1$ pour lequel on a :

$$0 < u_s - \frac{1}{2} < 10^{-2}$$

Pour cela, on pourra déterminer, avec une calculatrice, le signe de $f_n\left(\frac{1}{2} + \frac{1}{10^2}\right)$ pour $n = 2, 3, \cdots$, où f_n est la fonction définie par :

$$f_n(x) = x^n + x^{n-1} + \cdots + x - 1.$$

(b) Écrire en français une procédure, qui pour un entier $p \geq 1$ donné, permet de déterminer le plus petit entier s pour lequel on a :

$$0 < u_s - \frac{1}{2} \leq 10^{-p}$$

On pourra utiliser les fonctions g_n définies par :

$$g_n(x) = (x-1) f_n(x).$$

8. On se propose de montrer l'inégalité suivante valable pour tout entier $n \geq 1$:

$$u_n \leq \frac{1}{2} + \frac{1}{2n} \tag{4.2}$$

(a) En utilisant la fonction g_n définie dans la question **I.7.** démontrer que l'inégalité (4.2) est équivalente à l'inégalité suivante :

$$\frac{1}{2^{n+1}} \leq \frac{n^n}{(n+1)^{n+1}} \tag{4.3}$$

(b) Pour $x > 0$, on pose :

$$\psi(x) = (x+1)\ln(x+1) - x\ln(x) - (x+1)\ln(2).$$

Étudier la variation de la fonction ψ et en déduire l'inégalité (4.3).

9.

(a) Démontrer l'inégalité $\frac{1}{2} < u_4 < \frac{6}{11}$.

(b) En déduire que l'on a, pour tout entier $n \geq 4$, l'inégalité :

$$\frac{u_n}{2(1-u_n)} < \frac{n^{\frac{n}{n+1}}}{n+1}.$$

– II – Expression de u_n comme somme d'une série

Dans cette partie, on se propose d'établir, lorsque l'entier p est assez grand, l'expression suivante de u_p comme somme d'une série convergente :

$$u_p = \frac{1}{2} + \sum_{n=1}^{+\infty} \frac{1}{n \cdot 2^{n(p+1)+1}} \binom{n\,(p+1)}{n-1} \qquad (T_p)$$

1. Soit p un entier ≥ 1. On note S_p la série entière définie par :

$$S_p\,(x) = \sum_{n=1}^{+\infty} \frac{1}{2n} \binom{n\,(p+1)}{n-1} x^n$$

   (a) Démontrer que le rayon de convergence ρ_p de la série entière S_p est donné par :
$$\rho_p = \frac{p^p}{(p+1)^{p+1}}$$

   (b) Démontrer que, pour $p \geq 2$, la série du second membre de la relation (T_p) est convergente. (On utilisera la question **I.8.**).

2.

   (a) Démontrer, par récurrence sur l'entier $n \geq 1$, l'égalité :

$$\sum_{k=1}^{n} \frac{1}{k \cdot 2^{2k+1}} \binom{2k}{k-1} = \frac{1}{2} - \frac{2\,(n+2)}{(n+1)\,2^{2n+3}} \binom{2\,(n+1)}{n}$$

   (b) En déduire la relation (T_1).

3. On a admis dans les préliminaires que, pour tout entier $q \geq 1$, la série entière :
$$\sum_{n \geq 0} (-1)^n \binom{n+q-1}{n} x^n$$
a un rayon de convergence égal à 1, et que, pour tout $x \in \left]-1, 1\right[$, sa somme est égale à $\dfrac{1}{(1+x)^q}$.
En déduire, pour $n \geq 1$, $p \geq 1$ et $x \in \left]-1, 1\right[$, l'égalité : :

$$\frac{x^n}{(1+x)^{n(p+1)}} = \sum_{k=0}^{+\infty} (-1)^k \binom{n\,(p+1)+k-1}{k} x^{n+k}.$$

4. Pour $p \geq 1$, on pose :
$$v_p = 2u_p - 1.$$
   (a) Démontrer que l'on a :
$$\frac{v_p}{(1+v_p)^{p+1}} = \frac{1}{2^{p+1}}.$$
   (b) Déduire de ce qui précède que l'on a, pour $p \geq 2$ et $n \geq 1$, l'égalité :
$$\frac{1}{2^{n(p+1)}} = \sum_{k=0}^{+\infty} (-1)^k \binom{n(p+1)+k-1}{k} v_p^{n+k}.$$
5. **Dans toute la fin de cette deuxième partie, on fixe l'entier** $p \geq 4$, **et on pose :**
$$a_{n,k} = \frac{(-1)^k}{2n} \binom{n(p+1)+k-1}{k} \binom{n(p+1)}{n-1} v_p^{n+k}.$$
   (a) Démontrer la relation :
$$\sum_{n=1}^{+\infty} \frac{1}{n \cdot 2^{n(p+1)+1}} \binom{n(p+1)}{n-1} = \sum_{n=1}^{+\infty} \left(\sum_{k=0}^{+\infty} a_{n,k} \right).$$
   (b) Démontrer que, pour tout $n \geq 1$, la série $\sum_{k \geq 0} |a_{n,k}|$ est convergente et déterminer sa somme.
   (c) En utilisant les questions **I.9.** et **II.1.** démontrer que la série $\sum_{n=1}^{+\infty} \sum_{k=0}^{+\infty} |a_{n,k}|$ est convergente.
6. Soit q un entier ≥ 2 et $\mathbb{R}_{q-1}[X]$ le $\mathbb{R}$-espace vectoriel des polynômes à coefficients réels dont le degré est $\leq q-1$. On note Δ_q l'application qui, à un polynôme $P(X)$ de degré $\leq q-1$, associe le polynôme $P(X+1) - P(X)$.
   (a) Démontrer que Δ_q est un endomorphisme nilpotent de $\mathbb{R}_{q-1}[X]$.
   (b) En déduire que, si P est un polynôme de degré $\leq q-1$, on a :
$$\sum_{j=0}^{q} (-1)^{q-j} \binom{q}{j} P(X+j) = 0.$$
7.

(a) Soit toujours q un entier ≥ 2. En utilisant la question précédente, démontrer que la somme $\sum a_{n,k}$ étendue aux indices (n,k) tels que $n \geq 1$, $k \geq 0$ et $n+k=q+1$, est nulle.

(b) En déduire la relation (T_p) pour $p \geq 4$.

8. On fixe toujours l'entiers $p \geq 4$. Pour tout entier $n \geq 1$, on pose :

$$\lambda_n = \frac{1}{n \cdot 2^{n(p+1)+1}} \binom{n\,(p+1)}{n-1}.$$

(a) Démontrer l'existence d'un nombre réel μ_p appartenant à l'intervalle $]0,1[$ tel que l'on ait :

$$\lambda_{n+1} \backsim \mu_p \lambda_n \text{ lorsque } n \text{ tend vers } +\infty.$$

(b) Démontrer que la série $\sum\limits_{n \geq 1} \lambda_n$ est convergente et que son reste :

$$R_p\,(n) = \sum_{k=n+1}^{+\infty} \frac{1}{k \cdot 2^{k(p+1)+1}} \binom{k\,(p+1)}{k-1}$$

satisfait à l'équivalence $R_p\,(n) \sim \dfrac{\mu_p}{1-\mu_p}$ lorsque n tend vers $+\infty$.

– III – Réversion de Lagrange

Pour cette partie f et Φ désignent deux fonctions de classe $\mathcal{C}^\infty$ définies sur $\mathbb{R}$ et à valeurs réelles.
Pour z, t et $y \in \mathbb{R}$, on pose :

$$F\,(x,t,y) = t - y + x\Phi\,(y)\,.$$

1.

(a) En utilisant les rappels du préliminaire, démontrer qu'il existe un voisinage U de $(0,0)$ dans $\mathbb{R}^2$ et une fonction $\varphi : U \to \mathbb{R}$ de classe $\mathcal{C}^\infty$ telle que $\varphi\,(0,0) = 0$ et $F\,(x,t,\varphi\,(x,t)) = 0$ pour $(x,t) \in U$.

(b) Démontrer que l'on a dans U l'égalité :

$$\frac{\partial \varphi}{\partial x} = (\Phi \circ \varphi)\,\frac{\partial \varphi}{\partial t}.$$

2. On définit la fonction u dans U par $u = f \circ \varphi$.

(a) Vérifier que la fonction u est de classe $\mathcal{C}^\infty$ et satisfait à l'égalité :

$$\frac{\partial u}{\partial x} = (\Phi \circ \varphi) \frac{\partial u}{\partial t}.$$

(b) Plus généralement, démontrer, par récurrence sur $n \geq 1$, que l'on a :

$$\frac{\partial^n u}{\partial x^n} = \frac{\partial^{n-1}}{\partial t^{n-1}} \left((\Phi \circ \varphi)^n \frac{\partial u}{\partial t} \right).$$

(c) En déduire que l'on a, pour tout entier $n \geq 1$ et pour $(0, t) \in U$, l'égalité :

$$\frac{\partial^n u}{\partial x^n} (0, t) = \frac{d^{n-1}}{dt^{n-1}} \left((\Phi (t))^n f' (t) \right).$$

3. Soit $g : \mathbb{R} \to \mathbb{R}$ une fonction de classe $\mathcal{C}^\infty$ telle que $g (0) = 0$ et $g' (0) \neq 0$.

(a) Justifier que l'on peut définir une fonction σ dans un voisinage de 0 dans $\mathbb{R}$ par :

$$\sigma (s) = \begin{cases} \dfrac{s}{g (s)} & \text{si } s \neq 0 \\ \dfrac{1}{g' (0)} & \text{si } s = 0 \end{cases}$$

(b) Démontrer que la fonction σ est de classe $\mathcal{C}^1$ au voisinage de 0.

(c) Plus précisément, démontrer que la fonction σ est de classe $\mathcal{C}^\infty$ au voisinage de 0 dans $\mathbb{R}$. (Pour cela, on pourra calculer et utiliser l'intégrale $\displaystyle\int_0^1 g' (st)\, dt$).

4. Dans la fin de cette partie de problème, on conserve la fonction g de la question **III.3.** Expliquer l'existence d'un intervalle J, voisinage de 0 dans $\mathbb{R}$, et d'une fonction h de classe $\mathcal{C}^\infty$ sur $g (J)$, qui soit réciproque de la restriction de g à J.

5. Les résultats des questions **III.1. III.2.** restent valables lorsque la fonction Φ n'est définie que dans un voisinage de 0 dans $\mathbb{R}$ car d'emblée on n'a utilisé que des propriétés locales de la fonction Φ. On pourra utiliser ces résultats dans ce cadre plus étendu.
Dans cette question, on prend pour fonction f la fonction identique (caractérisée par $f (x) = x$) et pour fonction Φ la fonction σ définie dans la question **III.3.**

(a) Démontrer que l'on a alors $\varphi (x, 0) = h (x)$ pour x voisin de 0.

(b) Démontrer que, pour tout entier $n \geq 1$, les fonctions $\dfrac{d^n h}{dx^n}$ et $\dfrac{d^{n-1}(\sigma^n)}{dt^{n-1}}$ prennent la même valeur au point 0, c'est-à-dire :

$$\frac{d^n h}{dx^n}(0) = \frac{d^{n-1}(\sigma^n)}{dt^{n-1}}(0).$$

Cette formule constitue la formule de réversion de Lagrange.

6. Plus généralement, démontrer, pour tout entier $n \geq 1$ et toute fonction f de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$, la relation :

$$\frac{d^n (f \circ h)}{dx^n}(0) = \frac{d^{n-1}(\sigma^n f')}{dt^{n-1}}(0).$$

– IV – Application à la suite (u_n)

1. Pour $p \geq 1$ et $x \in \mathbb{R}$, $x \neq -1$, on pose :

$$\tau_p(x) = \frac{x}{(1+x)^{p+1}}.$$

Rappelons que ρ_p désigne le rayon de convergence de la série entière S_p calculé dans la question **II.1.**
Démontrer que la fonction τ_p réalise un homéomorphisme de l'intervalle $\left[0, \dfrac{1}{p}\right]$ sur l'intervalle $[0, \rho_p]$ et un difféomorphisme de classe $\mathcal{C}^\infty$ de l'intervalle $\left[0, \dfrac{1}{p}\right[$ sur l'intervalle $[0, \rho_p[$.

2. Pour $p \geq 1$, on note $w_p : [0, \rho_p] \to \mathbb{R}$ la fonction réciproque de la restriction de la fonction τ_p à l'intervalle $\left[0, \dfrac{1}{p}\right]$. Démontrer, à l'aide de la formule de réversion de Lagrange, que l'on a, pour tout entier $n \geq 1$:

$$\frac{w_p^{(n)}(0)}{n!} = \frac{1}{n}\binom{n(p+1)}{n-1}.$$

3. Soit $\sum\limits_{n \geq 1} a_n$ une série à termes > 0. On suppose qu'il existe un réel $\alpha > 1$ tel que l'on ait :

$$\frac{\alpha_{n+1}}{a_n} = 1 - \frac{\alpha}{n} + o\left(\frac{1}{n}\right).$$

On se propose de démontrer que la série $\sum\limits_{n \geq 1} a_n$ est convergente. Pour cela, on choisit un nombre réel β tel que $1 < \beta < \alpha$ et on considère la série de terme général $b_n = \dfrac{1}{n^\beta}$.

   (a) Dire pourquoi la série $\sum_{n\geq 1} b_n$ est convergente.
   (b) En déduire que la série $\sum_{n\geq 1} a_n$ est convergente.

4. On a introduit dans la question **II.1.** la série entière S_p définie par :

$$S_p(x) = \sum_{n=1}^{+\infty} \frac{1}{2n} \binom{n(p+1)}{n-1} x^n$$

   et on a calculé son rayon de convergence ρ_p.
   Démontrer que cette série est convergente sur tout l'intervalle $[-\rho_p, \rho_p]$.

5. On se propose de démontrer l'égalité $w_p = 2S_p$ sur l'intervalle $[0, \rho_p]$.
   (a) Démontrer que les fonctions $x \mapsto 2S_p(x) - x(1 + 2S_p(x))^{p+1}$ et $x \mapsto w_p(x) - x(1 + w_p(x))^{p+1}$ ont mêmes développements limités à tous ordres, au voisinage de 0.
   (b) En déduire que pour tout $x \in [0, \rho_p]$, on a :

$$2S_p(x) - x(1 + 2S_p(x))^{p+1} = 0.$$

   (c) En déduire que l'on a $w_p = 2S_p$ sur l'intervalle $[0, \rho_p]$.

6.
   (a) Vérifier que le nombre réel v_p défini dans la question **II.4.** appartient à l'intervalle $\left[0, \frac{1}{p}\right]$ pour $p \geq 1$.
   (b) Déduire de ce qui précède une autre démonstration, pour $p \geq 1$, de la relation :

$$u_p = \frac{1}{2} + \sum_{n=1}^{+\infty} \frac{1}{n \cdot 2^{n(p+1)+1}} \binom{n(p+1)}{n-1}$$

   de la partie **II** de l'énoncé.

4.2 Corrigé

– I – La suite (u_n)

1. Soit $f_n : x \mapsto x^n + x^{n-1} + \cdots + x - 1$.
   Pour $n = 1$, l'unique solution réelle de $f_1(x) = x - 1 = 0$ est $u_1 = 1$.
   Pour $n \geq 2$, la fonction f_n est continue sur $\mathbb{R}$ avec $f_n'(x) > 0$ pour $x \geq 0$,

$f_n(0) = -1 < 0$ et $f_n(1) = n - 1 > 0$, ce qui entraîne l'existence et l'unicité d'une racine positive $u_n \in \left]0, 1\right[$ de l'équation $f_n(x)$ (théorème des valeurs intermédiaires). Sur la figure 4.1, on a tracé les graphes de f_n pour $n = 1, 2, 3$ et 4 et il semble que la suite $(u_n)_{n\geq 1}$ converge vers $\frac{1}{2}$.

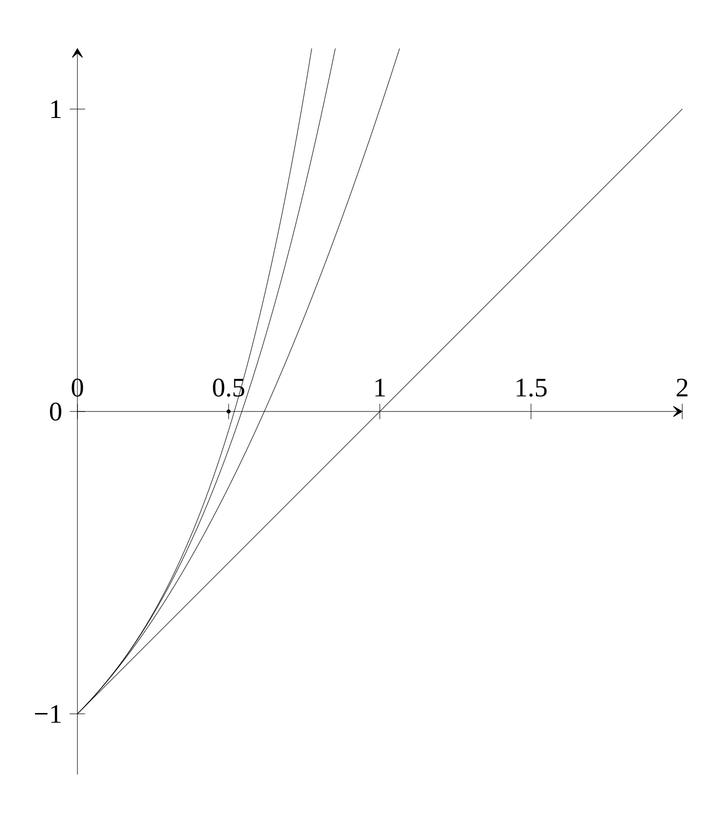


FIG. 4.1 – Graphes de f_1, f_2, f_3, f_4

2. De $f_{n+1}(u_{n+1}) = 0 = u_{n+1}^{n+1} + f_n(u_{n+1})$, on déduit que $f_n(u_{n+1}) = -u_{n+1}^{n+1} < 0$ et $0 < u_{n+1} < u_n \leq 1$. La suite $(u_n)_{n\in\mathbb{N}^*}$ est donc strictement décroissante minorée et en conséquence convergente vers un réel λ dans $\left[0, 1\right[$.
3. Pour $x \neq 1$, on a :

$$f_n(x) = \sum_{k=0}^{n} x^k - 2 = \frac{1 - x^{n+1}}{1 - x} - 2 = \frac{2x - 1 - x^{n+1}}{1 - x}$$

et pour $n \geq 2$, l'équation $f_n(u_n) = 0$ équivaut à $u_n^{n+1} - 2u_n + 1 = 0$ (dans ce cas, on a $0 < u_n < 1$).
Pour $n = 1$, on a $u_1 = 1$ et $u_1^2 - 2u_1 + 1 = 0$.

4.
   (a) u_2 est la solution positive de $x^2 + x - 1 = 0$, soit $u_2 = \dfrac{\sqrt{5} - 1}{2}$.
   (b) De $u_2 \in \,]0, 1[$ et $0 \leq u_n^{n+1} \leq u_2^{n+1}$ pour $n \geq 2$, on déduit que $\lim\limits_{n \to +\infty} \left(u_n^{n+1}\right) = 0$ et de $2u_n = u_n^{n+1} + 1 = 0$, on déduit que $\lim\limits_{n \to +\infty} (u_n) = \dfrac{1}{2}$.

5. De $2\varepsilon_n = 2u_n - 1 = u_n^{n+1}$ et $0 \leq nu_n^{n+1} \leq nu_2^{n+1}$ avec $u_2 \in \,]0, 1[\,$, pour $n \geq 2$, on déduit que $\lim\limits_{n \to +\infty} n\varepsilon_n = \lim\limits_{n \to +\infty} nu_n^{n+1} = \lim\limits_{n \to +\infty} nu_2^{n+1} = 0$.

6. On a :

$$2\varepsilon_n = 2u_n - 1 = u_n^{n+1} = \left(\varepsilon_n + \frac{1}{2}\right)^{n+1} = \frac{1}{2^{n+1}} (2\varepsilon_n + 1)^{n+1}$$

soit :

$$2^{n+2}\varepsilon_n = (2\varepsilon_n + 1)^{n+1} = e^{(n+1)\ln(2\varepsilon_n + 1)}$$

avec :

$$(n + 1) \ln (2\varepsilon_n + 1) = (n + 1) \ln (2\varepsilon_n + 1) \underset{n \to +\infty}{\sim} 2 (n + 1) \varepsilon_n$$

($\lim\limits_{n \to +\infty} \varepsilon_n = 0$). De $\lim\limits_{n \to +\infty} n\varepsilon_n = 0$, on déduit que $\lim\limits_{n \to +\infty} 2^{n+2}\varepsilon_n = 1$, c'est-à-dire que $\varepsilon_n \underset{n \to +\infty}{\sim} \dfrac{1}{2^{n+2}}$ ou encore :

$$\varepsilon_n = u_n - \frac{1}{2} = \frac{1}{2^{n+2}} + o\left(\frac{1}{2^n}\right).$$

7.
   (a) On a :

$$\begin{aligned} f_4\left(\frac{1}{2} + \frac{1}{10^2}\right) &= f_4\left(\frac{51}{100}\right) \\ &= \frac{51^4}{100^4} + \frac{51^3}{100^3} + \frac{51^2}{100^2} + \frac{51}{100} - 1 \\ &= -\frac{2959\,699}{100\,000\,000} \approx -2.959\,7 \times 10^{-2} < 0 = f_4(u_4) \end{aligned}$$

et :

$$\begin{aligned}
f_5\left(\frac{1}{2}+\frac{1}{10^2}\right) &= f_5\left(\frac{51}{100}\right) \\
&= \frac{51^5}{100^5}+\frac{51^4}{100^4}+\frac{51^3}{100^3}+\frac{51^2}{100^2}+\frac{51}{100}-1 \\
&= \frac{49\,055\,351}{10\,000\,000\,000} \approx 4.905\,5\times 10^{-3} > 0 = f_5(u_5)
\end{aligned}$$

et avec la stricte croissance des fonctions f_n sur $\mathbb{R}^+$, on déduit que :

$$u_5 < \frac{1}{2}+\frac{1}{10^2} < u_4$$

soit :

$$0 < u_5 - \frac{1}{2} < \frac{1}{10^2} < u_4 - \frac{1}{2}$$

et $s=5$ (la suite $(u_n)_{n\geq 1}$ est strictement décroissante).

(b) On a $g_n(x) = (x-1) f_n(x) = x^{n+1} - 2x + 1$ pour $n \geq 1$ et sur l'intervalle $[0,1]$ les fonctions f_n et g_n sont de signes contraires. Il s'agit alors de déterminer le plus petit entier $s \geq 2$ tel que $g_s\left(\frac{1}{2}+\frac{1}{10^p}\right) g_{s-1}\left(\frac{1}{2}+\frac{1}{10^p}\right) < 0$. Ce qui peut se faire avec la procédure suivante :

début
  $s = 1$;
  $x = \frac{1}{2}+\frac{1}{10^p}$;
  tant que $\left(x^{s+1}-2x+1\right)(x^s-2x+1) > 0$ faire
    $s = s+1$;
  fin tant que ;
fin

8. Pour $n=1$, on a l'égalité $u_1 = 1 = \frac{1}{2}+\frac{1}{2}$. Nous supposons que $n \geq 2$ et montrerons des inégalités strictes.

(a) f_n étant strictement croissante sur $[0,1]$, l'inégalité $u_n < \frac{1}{2}+\frac{1}{2n}$ est équivalente à $0 = f_n(u_n) < f_n\left(\frac{1}{2}+\frac{1}{2n}\right)$ qui est encore équivalente

à $g_n\left(\frac{1}{2}+\frac{1}{2n}\right)<0$ avec :

$$\begin{aligned} g_n\left(\frac{1}{2}+\frac{1}{2n}\right) &= \left(\frac{1}{2}+\frac{1}{2n}\right)^{n+1} - 2\left(\frac{1}{2}+\frac{1}{2n}\right)+1 \\ &= \frac{1}{2^{n+1}}\left(\frac{n+1}{n}\right)^{n+1} - \frac{1}{n} \end{aligned}$$

donc :

$$\begin{aligned} \left(u_n < \frac{1}{2}+\frac{1}{2n}\right) &\Leftrightarrow \left(\frac{1}{2^{n+1}}\left(\frac{n+1}{n}\right)^{n+1} < \frac{1}{n}\right) \\ &\Leftrightarrow \left(\frac{1}{2^{n+1}} < \frac{n^n}{(n+1)^{n+1}}\right) \end{aligned}$$

En notant $v_n = \frac{2^{n+1}n^n}{(n+1)^{n+1}}$, on a :

$$v_n = \frac{2^{n+1}}{n+1}\frac{1}{\left(1+\frac{1}{n}\right)^n} \underset{n\to+\infty}{\to} +\infty$$

et $v_n > 1$ pour n assez grand.

(b) L'inégalité $\frac{1}{2^{n+1}} < \frac{n^n}{(n+1)^{n+1}}$ pour $n \geq 2$ (pour $n = 1$ il y a égalité), est équivalente à :

$$\begin{aligned} \ln\left(\frac{1}{2^{n+1}}\right) &= -(n+1)\ln(2) \\ &< \ln\left(\frac{n^n}{(n+1)^{n+1}}\right) = n\ln(n) - (n+1)\ln(n+1) \end{aligned}$$

soit à :

$$\forall n \geq 2,\ (n+1)\ln(n+1) - n\ln(n) - (n+1)\ln(2) > 0$$

ce qui justifie l'introduction de la fonction ψ. Cette fonction est indéfiniment dérivable sur $\mathbb{R}^{+,*}$ avec :

$$\psi'(x) = \ln\left(\frac{x+1}{x}\right) - \ln(2)$$

$\lim_{x\to 0^+} \psi(x) = -\ln(2)$ et $\lim_{x\to +\infty} \psi(x) = -\infty$. Pour la limite à l'infini, on écrit que :

$$\psi(x) = x \ln\left(1 + \frac{1}{x}\right) + (x+1)\left(\frac{\ln(x+1)}{x+1} - \ln(2)\right) \underset{x\to+\infty}{\to} -\infty$$

La dérivée s'annule uniquement pour $x = 1$. On en déduit alors le tableau de variation de ψ et l'allure de son graphe, ce qui permet de déduire que ψ est strictement décroissante sur $[1, +\infty[$ et $\psi(x) > 0$ pour $x > 1$. L'inégalité (4.3) s'en déduit alors (figure 4.2). On a

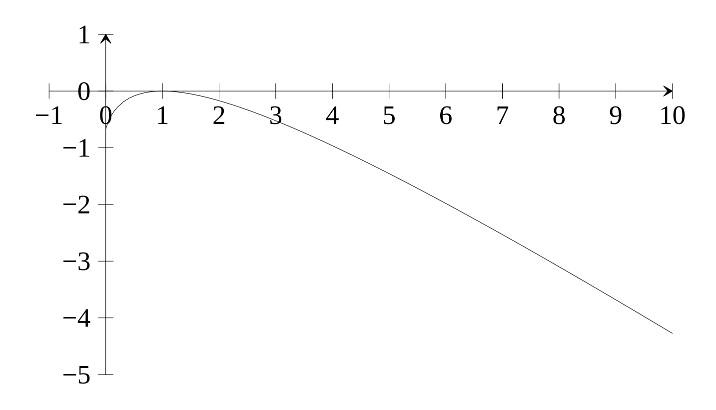


FIG. 4.2 – Graphe de ψ

donc :

$$\forall n \geq 2,\ \frac{1}{2} < u_n < \frac{1}{2} + \frac{1}{2n} < 1 = u_1$$

l'inégalité $\frac{1}{2} < u_n$ étant justifiée par le fait que la suite $(u_n)_{n\geq 1}$ converge en étant strictement décroissante vers $\frac{1}{2}$.

9.

(a) Pour $n = 4$, l'encadrement précédent donne, $\frac{1}{2} < u_4 < \frac{5}{8} \approx 0.625$. En fait u_4 est la solution dans $\left]\frac{1}{2}, 1\right[$ de $x^5 - 2x + 1 = 0$, soit $u_4 \approx 0.518\,79$ et on propose une majoration plus fine.
L'inégalité $u_4 < \frac{6}{11}$ est équivalente à $0 = f_4(u_4) < f_4\left(\frac{6}{11}\right)$ qui

est encore équivalente à $g_4\left(\frac{6}{11}\right) < 0$. Et on a bien :

$$g_4\left(\frac{6}{11}\right) = \left(\frac{6}{11}\right)^5 - 2\frac{6}{11} + 1 = -\frac{241\,121}{161\,051} < 0.$$

(b) La fonction $\varphi : x \mapsto \frac{x}{1-x}$ étant strictement croissante sur $]0,1[$ et la suite $(u_n)_{n\geq 1}$ décroissante, on a :

$$\forall n \geq 4,\ \frac{u_n}{2(1-u_n)} \leq \frac{u_4}{2(1-u_4)} < \frac{1}{2}\varphi\left(\frac{6}{11}\right) = \frac{3}{5}$$

et il suffit de montrer que $\frac{3}{5} < \frac{n^{\frac{n}{n+1}}}{n+1}$ pour tout $n \geq 4$, ce qui équivaut à :

$$g(n) = \frac{n}{n+1}\ln(n) - \ln(n+1) > \ln\left(\frac{3}{5}\right)$$

La fonction g est dérivable sur $\mathbb{R}^{+,*}$ avec :

$$g'(x) = \frac{\ln(x)}{(x+1)^2} > 0$$

pour $x > 1$. On a donc, pour $n \geq 4$:

$$g(n) \geq g(4) = \frac{4\ln(4) - 5\ln(5)}{5} = \frac{\ln\left(\frac{4^4}{5^5}\right)}{5} > \ln\left(\frac{3}{5}\right)$$

(c'est une conséquence de $\ln\left(\frac{4^4}{5^5}\right) > 5\ln\left(\frac{3}{5}\right) = \ln\left(\frac{3^5}{5^5}\right)$ qui est encore équivalent à $4^4 = 256 > 3^5 = 243$ qui est vrai).

– II – Expression de u_n comme somme d'une série

1. On note $a_n = \frac{1}{2n}\binom{n(p+1)}{n-1}$ pour $n \geq 1$ et p fixé.

(a) Avec $a_n > 0$ et :

$$\begin{aligned}\frac{a_{n+1}}{a_n} &= \frac{n}{n+1}\frac{((n+1)(p+1))!}{n!\,((n+1)(p+1)-n)!}\frac{(n-1)!\,(n(p+1)-(n-1))!}{(n(p+1))!} \\ &= \frac{1}{n+1}\frac{(n(p+1)+(p+1))!}{(n(p+1))!}\frac{(np+1)!}{(np+1+p)!} \\ &= \frac{1}{n+1}\frac{(n(p+1)+(p+1))\cdots(n(p+1)+1)}{(np+1+p)\cdots(np+2)} \\ &= \frac{1}{n+1}\frac{(p+1)^{p+1}n^{p+1}+\cdots+(p+1)!}{p^pn^p+\cdots+(p+1)!}\end{aligned}$$

on déduit que :

$$\frac{a_{n+1}}{a_n} \underset{n\to+\infty}{\sim} \frac{1}{n}\frac{(p+1)^{p+1}n^{p+1}}{p^pn^p} = \frac{(p+1)^{p+1}}{p^p}$$

et le théorème de d'Alembert nous dit que le rayon de convergence de la série entière S_p est $\rho_p = \dfrac{p^p}{(p+1)^{p+1}}$.

(b) L'inégalité $\dfrac{1}{2^{p+1}} < \rho_p = \dfrac{p^p}{(p+1)^{p+1}}$ valable pour $p \geq 2$ (question **I.8.b.**) nous dit que la série S_p converge pour $x = \dfrac{1}{2}$, ce qui valide la convergence de la série du second membre de (T_p).

2. On note :

$$S_n = \sum_{k=1}^{n} \frac{1}{k\cdot 2^{2k+1}}\binom{2k}{k-1}$$

(a) Pour $n = 1$, on a

$$S_1 = \frac{1}{2^3}\binom{2}{0} = \frac{1}{8} = \frac{1}{2} - \frac{2\cdot 3}{2\cdot 2^5}\binom{2\cdot 2}{1}.$$

Supposant le résultat acquis au rang $n \geq 1$, on a :

$$\begin{aligned}S_{n+1} &= S_n + \frac{1}{(n+1)\cdot 2^{2n+3}}\binom{2(n+1)}{n} \\ &= \frac{1}{2} - \frac{2(n+2)}{(n+1)\,2^{2n+3}}\binom{2(n+1)}{n} + \frac{1}{(n+1)\cdot 2^{2n+3}}\binom{2(n+1)}{n} \\ &= \frac{1}{2} + \frac{1}{(n+1)\cdot 2^{2n+3}}\binom{2(n+1)}{n}(1-2(n+2)) \\ &= \frac{1}{2} - \frac{2n+3}{(n+1)\cdot 2^{2n+3}}\binom{2(n+1)}{n}\end{aligned}$$

et compte tenu de :

$$\begin{aligned}\binom{2(n+2)}{n+1} &= \frac{(2(n+2))!}{(n+1)!\,(n+3)!} = \frac{(2n+4)(2n+3)}{(n+1)(n+3)}\frac{(2(n+1))!}{n!\,(n+2)!}\\ &= \frac{(2n+4)(2n+3)}{(n+1)(n+3)}\binom{2(n+1)}{n}\end{aligned}$$

il vient :

$$\begin{aligned}S_{n+1} &= \frac{1}{2} - \frac{2n+3}{(n+1)\cdot 2^{2n+3}}\frac{(n+1)(n+3)}{(2n+4)(2n+3)}\binom{2(n+2)}{n+1}\\ &= \frac{1}{2} - \frac{2(n+3)}{2^{2n+5}(n+2)}\binom{2(n+2)}{n+1}\end{aligned}$$

soit le résultat au rang $n+1$.
On a donc :

$$\begin{aligned}S_n &= \sum_{k=1}^{n}\frac{1}{k\cdot 2^{2k+1}}\binom{2k}{k-1} = \frac{1}{2} - \frac{2(n+2)}{(n+1)\,2^{2n+3}}\binom{2(n+1)}{n}\\ &= \frac{1}{2} - \frac{2(n+2)}{(n+1)\,2^{2n+3}}\frac{(2(n+1))!}{n!\,(n+2)!}\\ &= \frac{1}{2} - \frac{1}{2^{2n+2}}\frac{(2(n+1))!}{((n+1)!)^2}\end{aligned}$$

(b) Il s'agit de montrer que :

$$1 = u_1 = \frac{1}{2} + \sum_{n=1}^{+\infty}\frac{1}{n\cdot 2^{2n+1}}\binom{2n}{n-1}$$

soit que $\lim\limits_{n\to+\infty} S_n = \dfrac{1}{2}$ ou encore que $\lim\limits_{n\to+\infty} R_{n+1} = 0$, où on a noté $R_n = \dfrac{1}{2^{2n}}\dfrac{(2n)!}{(n!)^2}$. En utilisant la formule de Stirling, on a :

$$R_n \underset{n\to+\infty}{\backsim} \frac{1}{2^{2n}}\frac{(2n)^{2n}\,e^{-2n}\sqrt{2\pi 2n}}{n^{2n}e^{-2n}2\pi n} = \frac{1}{\sqrt{\pi}\sqrt{n}} \underset{n\to+\infty}{\to} 0.$$

3. En utilisant le développement en série entière sur $]-1,1[$:

$$\frac{1}{(1+x)^q} = (1+x)^{-q} = \sum_{k=0}^{+\infty}(-1)^k\binom{q+k-1}{k}x^k$$

on a pour $n \geq 1$, $p \geq 1$ et $x \in \left]-1,1\right[$:

$$\frac{x^n}{(1+x)^{n(p+1)}} = \sum_{k=0}^{+\infty} (-1)^k \binom{n(p+1)+k-1}{k} x^{n+k}$$

4. Avec $g_n(x) = (x-1) f_n(x) = x^{n+1} - 2x + 1$, on déduit que pour $n \geq 2$, le réel u_n est solution dans $\left]0,1\right[$ de $x^{n+1} - 2x + 1$. Pour $n = 1$, $u_1 = 1$ est aussi solution de cette équation.

   (a) Pour $p \geq 1$, l'équation $u_p^{p+1} - 2u_p + 1 = 0$ s'écrit :

   $$v_p = 2u_p - 1 = u_p^{p+1} = \left(\frac{v_p+1}{2}\right)^{p+1}$$

   ou encore :

   $$\frac{v_p}{(1+v_p)^{p+1}} = \frac{1}{2^{p+1}}$$

   $(1 + v_p = 2u_p > 0)$.

   (b) Pour $n \geq 1$, on a $\dfrac{v_p^n}{(1+v_p)^{(p+1)n}} = \dfrac{1}{2^{(p+1)n}}$ et pour $p \geq 2$, on a $\dfrac{1}{2} < u_p < 1$, $v_p = 2u_p - 1 \in \left]0,1\right[$, donc :

   $$\frac{1}{2^{(p+1)n}} = \frac{v_p^n}{(1+v_p)^{(p+1)n}} = \sum_{k=0}^{+\infty} (-1)^k \binom{n(p+1)+k-1}{k} v_p^{n+k}.$$

5.

   (a) En utilisant le résultat précédent, on a :

   $$\begin{aligned}\sum_{n=1}^{+\infty} \frac{\binom{n(p+1)}{n-1}}{n2^{(p+1)n+1}} &= \sum_{n=1}^{+\infty} \frac{\binom{n(p+1)}{n-1}}{2n} \sum_{k=0}^{+\infty} (-1)^k \binom{n(p+1)+k-1}{k} v_p^{n+k} \\ &= \sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty} \frac{(-1)^k}{2n} \binom{n(p+1)}{n-1} \binom{n(p+1)+k-1}{k} v_p^{n+k} \\ &= \sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty} a_{n,k}\end{aligned}$$

(b) Comme $0 < v_p < 1$ pour $p \geq 2$, on peut utiliser **II.3.** pour écrire :

$$\begin{aligned}\frac{v_p^n}{(1-v_p)^{n(p+1)}} &= (-1)^n \frac{(-v_p)^n}{(1-v_p)^{n(p+1)}} \\ &= (-1)^n \sum_{k=0}^{+\infty} (-1)^k \binom{n(p+1)+k-1}{k} (-v_p)^{n+k} \\ &= \sum_{k=0}^{+\infty} \binom{n(p+1)+k-1}{k} v_p^{n+k}\end{aligned}$$

ce qui donne :

$$\begin{aligned}\frac{1}{2n}\binom{n(p+1)}{n-1}\frac{v_p^n}{(1-v_p)^{n(p+1)}} &= \frac{\binom{n(p+1)}{n-1}}{2n}\sum_{k=0}^{+\infty}\binom{n(p+1)+k-1}{k} v_p^{n+k} \\ &= \sum_{k=0}^{+\infty} \frac{\binom{n(p+1)}{n-1}\binom{n(p+1)+k-1}{k}}{2n} v_p^{n+k} \\ &= \sum_{k=0}^{+\infty} |a_{n,k}|\end{aligned}$$

d'où la convergence et la somme de la série $\sum |a_{n,k}|$.

(c) On a $\sum\limits_{k=0}^{+\infty} |a_{n,k}| = \dfrac{1}{2n}\dbinom{n(p+1)}{n-1} x^n$ avec $x = \dfrac{v_p}{(1-v_p)^{p+1}}$ et il s'agit de montrer que x est dans l'intervalle de convergence $]-\rho_p, \rho_p[$ de la série entière S_p, où $\rho_p = \dfrac{p^p}{(p+1)^{p+1}}$. Le **I.9.** nous dit que pour $p \geq 4$ on a, $0 < \dfrac{u_p}{2(1-u_p)} < \dfrac{p^{\frac{p}{p+1}}}{p+1}$ et tenant compte de $u_p^{p+1} - 2u_p + 1 = 0$, on en déduit que :

$$\begin{aligned}0 < \frac{v_p}{(1-v_p)^{p+1}} &= \frac{2u_p - 1}{2^{p+1}(1-u_p)^{p+1}} \\ &= \left(\frac{u_p}{2(1-u_p)}\right)^{p+1} < \frac{p^p}{(p+1)^{p+1}} = \rho_p\end{aligned}$$

et :

$$\begin{aligned}\sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty} |a_{n,k}| &= \sum_{n=1}^{+\infty} \frac{1}{2n}\binom{n(p+1)}{n-1}\frac{v_p^n}{(1-v_p)^{(p+1)n}} \\ &= S_p\left(\frac{v_p}{(1-v_p)^{p+1}}\right)\end{aligned}$$

6.

(a) On vérifie facilement que $\Delta_q : P \mapsto P(X+1) - P(X)$ est une application linéaire de $\mathbb{R}_{q-1}[X]$ dans $\mathbb{R}_{q-2}[X]$. Le degré étant diminué de 1 à chaque étape, on a $\Delta_q^q = 0$.

(b) En désignant par τ l'application linéaire $\tau : P \mapsto P(X+1)$, on a $\Delta_q = \tau - I_d$ et :

$$\Delta_q^q = (\tau - I_d)^q = \sum_{j=0}^{q} (-1)^{q-j} \binom{q}{j} \tau^j$$

(τ et I_d commutent) avec $\tau^j : P \mapsto P(X+j)$. L'égalité $\Delta_q^q = 0$ se traduit alors par :

$$\sum_{j=0}^{q} (-1)^{q-j} \binom{q}{j} P(X+j) = 0$$

pour tout polynôme $P \in \mathbb{R}_{q-1}[X]$.

7.

(a) En notant $I_q = \{(n,k) \in \mathbb{N}^* \times \mathbb{N} \mid n+k = q+1\}$, on a :

$$\begin{aligned}\sum_{(n,k)\in I_q} a_{n,k} &= \sum_{(n,k)\in I_q} \frac{(-1)^k}{2n} \binom{n(p+1)}{n-1} \binom{n(p+1)+k-1}{k} v_p^{n+k} \\ &= \frac{v_p^{q+1}}{2} \sum_{(n,k)\in I_q} \frac{(-1)^k}{n} \binom{n(p+1)}{n-1} \binom{np+q}{k}\end{aligned}$$

avec :

$$\begin{aligned}\binom{n(p+1)}{n-1}\binom{np+q}{k} &= \frac{(n(p+1))!}{(n-1)!\,(np+1)!} \frac{(np+q)!}{k!\,(np+q-k)!} \\ &= \frac{(n(p+1))!}{(n-1)!\,(np+1)!} \frac{(np+q)!}{k!\,(n(p+1)-1)!} \\ &= \frac{n(p+1)}{(n-1)!\,(np+1)!} \frac{(np+q)!}{(q+1-n)!} \\ &= n(p+1)(np+q)\cdots(np+2) \frac{1}{(n-1)!} \frac{1}{(q+1-n)!} \\ &= \frac{n(p+1)(np+q)\cdots(np+2)}{q!} \binom{q}{n-1}\end{aligned}$$

ce qui donne :

$$\begin{aligned}\sum_{(n,k)\in I_q} a_{n,k} &= \frac{v_p^{q+1}}{2}\frac{p+1}{q!}\sum_{(n,k)\in I_q}(-1)^k\binom{q}{n-1}(np+q)\cdots(np+2)\\ &= \frac{v_p^{q+1}}{2}\frac{p+1}{q!}\sum_{(n,k)\in I_q}(-1)^{q+1-n}\binom{q}{n-1}(np+q)\cdots(np+2)\\ &= \frac{v_p^{q+1}}{2}\frac{p+1}{q!}\sum_{n=1}^{q+1}(-1)^{q+1-n}\binom{q}{n-1}(np+q)\cdots(np+2)\\ &= \frac{v_p^{q+1}}{2}\frac{p+1}{q!}\sum_{j=0}^{q}(-1)^{q-j}\binom{q}{j}((j+1)p+q)\cdots((j+1)p+2)\end{aligned}$$

soit en notant $P(X)=(pX+q)\cdots(pX+2)$ dans $\mathbb{R}_{q-1}[X]$:

$$\sum_{(n,k)\in I_q} a_{n,k} = \frac{v_p^{q+1}}{2}\frac{p+1}{q!}\sum_{j=0}^{q}(-1)^{q-j}\binom{q}{j}P(1+j)=0.$$

(b) La famille $(a_{n,k})_{(n,k)\in\mathbb{N}^*\times\mathbb{N}}$ étant sommable (question **II.5.b.**), on peut écrire :

$$\sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty}a_{n,k}=\sum_{r=1}^{+\infty}\sum_{\substack{(n,k)\in\mathbb{N}^*\times\mathbb{N}\\ n+k=r}}a_{n,k}$$

et la question précédente nous dit que, pour $p\geq 4$, la somme du second membre est réduite à $r\in\{1,2\}$ (puisque les $\sum_{(n,k)\in I_q} a_{n,k}$ sont nulles pour $q\geq 2$), ce qui donne :

$$\begin{aligned}\sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty}a_{n,k} &= a_{1,0}+a_{1,1}+a_{2,0}\\ &= \frac{v_p}{2}+\frac{-1}{2}\binom{p+1}{1}v_p^2+\frac{1}{4}\binom{2(p+1)}{1}v_p^2\\ &= \frac{v_p}{2}+\frac{v_p^2}{2}\left(\frac{1}{2}2(p+1)-(p+1)\right)=\frac{v_p}{2}\end{aligned}$$

et :

$$\sum_{n=1}^{+\infty}\frac{1}{n\cdot 2^{n(p+1)+1}}\binom{n(p+1)}{n-1}=\sum_{n=1}^{+\infty}\sum_{k=0}^{+\infty}a_{n,k}=\frac{v_p}{2}=u_p-\frac{1}{2}$$

soit :

$$\frac{1}{2}+\sum_{n=1}^{+\infty}\frac{1}{n\cdot 2^{n(p+1)+1}}\binom{n\,(p+1)}{n-1}=u_p.$$

8.

(a) En utilisant les coefficients $a_n=\dfrac{1}{2n}\dbinom{n\,(p+1)}{n-1}$ du **II.1.** on a $\lambda_n=\dfrac{a_n}{2^{n(p+1)}}$ et :

$$\frac{\lambda_{n+1}}{\lambda_n}=\frac{1}{2^{p+1}}\frac{a_{n+1}}{a_n}\underset{n\to+\infty}{\sim}\frac{1}{2^{p+1}}\frac{(p+1)^{p+1}}{p^p}=\frac{1}{2^{p+1}\rho_p}$$

En **II.1.b.** on a vu que $0<\dfrac{1}{2^{p+1}}<\rho_p$, ce qui entraîne $\mu_p=\dfrac{1}{2^{p+1}\rho_p}\in\left]0,1\right[$.

(b) Comme $\lim\limits_{n\to+\infty}\dfrac{\lambda_{n+1}}{\lambda_n}=\mu_p\in\left]0,1\right[$, le théorème de d'Alembert nous dit que la série $\sum\lambda_n$ est convergente (tous les λ_n sont strictement positifs). Avec $\lambda_{n+1}\underset{n\to+\infty}{\sim}\mu_p\lambda_n$ et la convergence des séries à termes positifs considérées, on déduit que $\sum\limits_{k=n}^{+\infty}\lambda_{k+1}\underset{n\to+\infty}{\sim}\mu_p\sum\limits_{k=n}^{+\infty}\lambda_k$, soit $R_p\,(n)\underset{n\to+\infty}{\sim}\mu_pR_p\,(n-1)$ et :

$$\lambda_n=R_p\,(n-1)-R_p\,(n)=R_p\,(n)\left(\frac{R_p\,(n-1)}{R_p\,(n)}-1\right)$$

avec $\lim\limits_{n\to+\infty}\dfrac{R_p\,(n-1)}{R_p\,(n)}=\dfrac{1}{\mu_p}>1$, ce qui donne :

$$\lambda_n\underset{n\to+\infty}{\sim}R_p\,(n)\left(\frac{1}{\mu_p}-1\right)=\frac{1-\mu_p}{\mu_p}R_p\,(n)\,.$$

– III – Réversion de Lagrange

1.

(a) Comme Φ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}$, la fonction F est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^3$. De plus, on a $F\,(0,0,0)=0$ et $\dfrac{\partial F}{\partial y}\,(0,0,0)=-1\neq 0$. On déduit

alors du théorème des fonctions implicites qu'il existe un voisinage ouvert U de $(0,0)$ dans $\mathbb{R}^2$, un voisinage ouvert V de 0 dans $\mathbb{R}$ et une fonction $\varphi : U \to V$ de classe $\mathcal{C}^\infty$ tels que :

$$\forall (x,t) \in U,\ \forall z \in V,\ (F(x,t,z) = 0 \Leftrightarrow z = \varphi(x,t)).$$

De $F(0,0,0) = 0$, on déduit que $\varphi(0,0) = 0$ et pour tout $(x,t) \in U$, on a $F(x,t,\varphi(x,t)) = 0$.

(b) Le théorème des fonctions implicites nous dit aussi que pour tout $(x,t) \in U$, on a :

$$\frac{\partial \varphi}{\partial x}(x,t) = -\frac{\frac{\partial F}{\partial x}(x,t,\varphi(x,t))}{\frac{\partial F}{\partial z}(x,t,\varphi(x,t))} = \frac{\Phi(\varphi(x,t))}{1 - x\Phi'(\varphi(x,t))}$$

et :

$$\frac{\partial \varphi}{\partial t}(x,t) = -\frac{\frac{\partial F}{\partial t}(x,t,\varphi(x,t))}{\frac{\partial F}{\partial z}(x,t,\varphi(x,t))} = \frac{1}{1 - x\Phi'(\varphi(x,t))}$$

ce qui donne :

$$\frac{\partial \varphi}{\partial x}(x,t) = \Phi(\varphi(x,t))\frac{\partial \varphi}{\partial t}(x,t).$$

2.

(a) La fonction u est de classe $\mathcal{C}^\infty$ sur U comme composée de deux fonctions de classe $\mathcal{C}^\infty$ et le théorème de différentiation des fonctions composées nous donne :

$$\begin{aligned}\frac{\partial u}{\partial x}(x,t) &= f'(\varphi(x,t))\frac{\partial \varphi}{\partial x}(x,t) = f'(\varphi(x,t))\,\Phi(\varphi(x,t))\frac{\partial \varphi}{\partial t}(x,t)\\ &= \Phi(\varphi(x,t))\frac{\partial u}{\partial t}(x,t)\end{aligned}$$

(b) Le **a.** nous dit que le résultat est vrai pour $n = 1$. Le supposant acquis pour $n - 1 \geq 1$, on a, en utilisant le théorème de Schwartz sur les dérivées partielles des fonctions $\mathcal{C}^\infty$:

$$\begin{aligned}\frac{\partial^n u}{\partial x^n} &= \frac{\partial}{\partial x}\left(\frac{\partial^{n-1} u}{\partial x^{n-1}}\right) = \frac{\partial}{\partial x}\left(\frac{\partial^{n-2}}{\partial t^{n-2}}\left((\Phi\circ\varphi)^{n-1}\frac{\partial u}{\partial t}\right)\right)\\ &= \frac{\partial^{n-2}}{\partial t^{n-2}}\left(\frac{\partial}{\partial x}\left((\Phi\circ\varphi)^{n-1}\frac{\partial u}{\partial t}\right)\right)\end{aligned}$$

avec :

$$\begin{aligned}
&\tfrac{\partial}{\partial x}\left((\Phi\circ\varphi)^{n-1}\tfrac{\partial u}{\partial t}\right)\\
&=\tfrac{\partial}{\partial x}\left((\Phi\circ\varphi)^{n-1}\right)\tfrac{\partial u}{\partial t}+(\Phi\circ\varphi)^{n-1}\tfrac{\partial}{\partial x}\left(\tfrac{\partial u}{\partial t}\right)\\
&=(n-1)\,(\Phi\circ\varphi)^{n-2}\left(\Phi'\circ\varphi\right)\tfrac{\partial\varphi}{\partial x}\tfrac{\partial u}{\partial t}+(\Phi\circ\varphi)^{n-1}\tfrac{\partial}{\partial t}\left(\tfrac{\partial u}{\partial x}\right)
\end{aligned}$$

et tenant compte de :

$$\frac{\partial\varphi}{\partial x}=\Phi\circ\varphi\frac{\partial\varphi}{\partial t}$$

$$\begin{aligned}
\frac{\partial}{\partial t}\left(\frac{\partial u}{\partial x}\right)=\frac{\partial}{\partial t}\left(\Phi\circ\varphi\frac{\partial u}{\partial t}\right)&=\frac{\partial}{\partial t}(\Phi\circ\varphi)\frac{\partial u}{\partial t}+\Phi\circ\varphi\frac{\partial^2 u}{\partial t^2}\\
&=\left(\Phi'\circ\varphi\right)\frac{\partial\varphi}{\partial t}\frac{\partial u}{\partial t}+\Phi\circ\varphi\frac{\partial^2 u}{\partial t^2}
\end{aligned}$$

cela donne :

$$\begin{aligned}
\frac{\partial}{\partial x}\left((\Phi\circ\varphi)^{n-1}\frac{\partial u}{\partial t}\right)&=(n-1)\,(\Phi\circ\varphi)^{n-1}\left(\Phi'\circ\varphi\right)\frac{\partial\varphi}{\partial t}\frac{\partial u}{\partial t}\\
&\quad+(\Phi\circ\varphi)^{n-1}\left(\Phi'\circ\varphi\right)\frac{\partial\varphi}{\partial t}\frac{\partial u}{\partial t}+(\Phi\circ\varphi)^{n}\frac{\partial^2 u}{\partial t^2}\\
&=n\,(\Phi\circ\varphi)^{n-1}\left(\Phi'\circ\varphi\right)\frac{\partial\varphi}{\partial t}\frac{\partial u}{\partial t}+(\Phi\circ\varphi)^{n}\frac{\partial^2 u}{\partial t^2}\\
&=\frac{\partial}{\partial t}\left((\Phi\circ\varphi)^{n}\frac{\partial u}{\partial t}\right)
\end{aligned}$$

et :

$$\frac{\partial^n u}{\partial x^n}=\frac{\partial^{n-2}}{\partial t^{n-2}}\left(\frac{\partial}{\partial x}\left((\Phi\circ\varphi)^{n-1}\frac{\partial u}{\partial t}\right)\right)=\frac{\partial^{n-1}}{\partial t^{n-1}}\left((\Phi\circ\varphi)^{n}\frac{\partial u}{\partial t}\right)$$

soit le résultat pour n.

(c) L'évaluation en $(0,t)\in U$, nous donne :

$$\begin{aligned}
\frac{\partial^n u}{\partial x^n}(0,t)&=\frac{\partial^{n-1}}{\partial t^{n-1}}\left((\Phi\circ\varphi)^{n}\frac{\partial u}{\partial t}\right)(0,t)\\
&=\frac{d^{n-1}}{dt^{n-1}}\left((\Phi(\varphi(0,t)))^{n}\frac{\partial u}{\partial t}(0,t)\right)
\end{aligned}$$

avec :

$$F(0,t,\varphi(0,t))=t-\varphi(0,t)=0$$

et :

$$\frac{\partial u}{\partial t}(0,t) = f'(\varphi(0,t))\frac{\partial \varphi}{\partial t}(0,t),$$

ce qui donne $\varphi(0,t) = t$, $\dfrac{\partial u}{\partial t}(0,t) = f'(t)$ et :

$$\frac{\partial^n u}{\partial x^n}(0,t) = \frac{d^{n-1}}{dt^{n-1}}\left((\Phi(t))^n f'(t)\right).$$

3.

(a) Comme $g'(0) \neq 0$ avec g' continue sur $\mathbb{R}$, il existe un réel $\delta > 0$ tel que $g'(x) \neq 0$ sur $]-\delta,\delta[$, le signe de g' étant constant sur cet intervalle. Pour tout réel $x \in]-\delta,\delta[$, on a alors :

$$g(x) = \int_0^x g'(t)\,dt + g(0) = \int_0^x g'(t)\,dt$$

avec $g(x) \neq 0$ pour $x \neq 0$. On peut donc définir la fonction σ sur $]-\delta,\delta[$ par :

$$\sigma(s) = \begin{cases} \dfrac{s}{g(s)} & \text{si } s \neq 0 \\ \dfrac{1}{g'(0)} & \text{si } s = 0 \end{cases}$$

(b) La fonction σ est de classe $\mathcal{C}^\infty$ sur $]-\delta,\delta[\setminus\{0\}$ comme quotient de deux fonctions $\mathcal{C}^\infty$, le dénominateur ne s'annulant jamais. Par définition du nombre dérivé, on a :

$$\lim_{\substack{x\to 0\\ x\neq 0}} \frac{g(x)}{x} = \lim_{\substack{x\to 0\\ x\neq 0}} \frac{g(x)-g(0)}{x} = g'(0) \neq 0,$$

donc $\lim\limits_{x\to 0} \sigma(x) = \dfrac{1}{g'(0)} = \sigma(0)$ et σ est continue en 0. De plus sur $]-\delta,\delta[\setminus\{0\}$, on a :

$$\sigma'(x) = \frac{g(x) - xg'(x)}{g^2(x)}$$

et utilisant la formule de Taylor Lagrange entre x et 0, on a :

$$g(0) = g(x) - xg'(x) + \frac{x^2}{2}g''(\theta_x x)$$

avec $0 < \theta_x < 1$, ce qui donne :

$$\begin{aligned}\sigma'(x) &= \frac{g(0) - \frac{x^2}{2} g''(\theta_x x)}{g^2(x)} \\ &= -\frac{g''(\theta_x x)}{2}\left(\frac{x}{g(x)}\right)^2 \underset{x\to 0}{\to} -\frac{g''(0)}{2}(\sigma(0))^2 = -\frac{g''(0)}{2(g'(0))^2}\end{aligned}$$

On déduit alors du théorème des accroissement finis que σ est dérivable en 0 de dérivée $\sigma'(0) = -\frac{g''(0)}{2(g'(0))^2}$, puis que σ' est continue en 0.
La fonction σ est donc de classe $\mathcal{C}^1$ sur $]-\delta, \delta[$.

(c) En fait avec $g(x) = \int_0^x g'(t)\,dt = x\int_0^1 g'(xu)\,du$, on a, sur $]-\delta, \delta[$:

$$\sigma(x) = \frac{1}{\int_0^1 g'(xu)\,du}$$

la fonction $x \mapsto \int_0^1 g'(xu)\,du$ étant de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^2$ (la fonction $(x,u) \mapsto g'(xu)$ est $\mathcal{C}^\infty$ sur $\mathbb{R}^2$ et on intègre sur un segment) ne s'annulant pas sur $]-\delta, \delta[$. Il en résulte que σ est de classe $\mathcal{C}^\infty$ sur $]-\delta, \delta[$.

4. La fonction g est de classe $\mathcal{C}^\infty$ sur $J =]-\delta, \delta[$ avec g' ne s'annulant jamais et de signe constant sur cet intervalle, elle est donc $\mathcal{C}^\infty$ strictement monotone sur J et réalise un $\mathcal{C}^\infty$-difféomorphisme de J sur $g(J)$.

5.

(a) Comme $\Phi = \sigma$ est de classe $\mathcal{C}^\infty$ sur $J =]-\delta, \delta[$, la fonction F définie par $F(x,t,y) = t - y + x\sigma(y)$ est de classe $\mathcal{C}^\infty$ sur $\mathbb{R}^2 \times J$. De plus, on a $F(0,0,0) = 0$ et $\frac{\partial F}{\partial y}(0,0,0) = -1 \neq 0$. On déduit alors du théorème des fonctions implicites qu'il existe un voisinage ouvert U de $(0,0)$ dans $\mathbb{R}^2$, un voisinage ouvert V de 0 dans J et une fonction $\varphi : U \to V$ de classe $\mathcal{C}^\infty$ tels que :

$$\forall (x,t) \in U,\ \forall y \in V,\ (F(x,t,y) = 0 \Leftrightarrow y = \varphi(x,t)).$$

En désignant par $r > 0$ un réel tel que $(x,0) \in U$ pour $|x| < r$, on a :

$$F(x,0,\varphi(x,0)) = 0 \Leftrightarrow \varphi(x,0) = x\sigma(\varphi(x,0))$$

avec $\sigma(\varphi(x,0)) \neq 0$. On a donc, pour $|x| < r$:

$$g(\varphi(x,0)) = \frac{\varphi(x,0)}{\sigma(\varphi(x,0))} = x$$

et considérant que g est un $\mathcal{C}^{\infty}$-difféomorphisme de J sur $g(J)$, on a :

$$\varphi(x,0) = g^{-1}(x) = h(x).$$

(b) En posant comme en **III.2.** $u = f \circ \varphi = \varphi$, on a pour $(0,t) \in U$:

$$\frac{\partial^n \varphi}{\partial x^n}(0,t) = \frac{\partial^n u}{\partial x^n}(0,t) = \frac{d^{n-1}}{dt^{n-1}}\left((\Phi(t))^n f'(t)\right) = \frac{d^{n-1}}{dt^{n-1}}\left((\sigma(t))^n\right).$$

et l'évaluation en $(0,0)$ donne :

$$\frac{\partial^n \varphi}{\partial x^n}(0,0) = \frac{d^{n-1}}{dt^{n-1}}(\sigma^n)(0)$$

D'autre part, de $\varphi(x,0) = h(x)$, pour $|x| < r$, on déduit que :

$$\frac{\partial^n \varphi}{\partial x^n}(x,0) = \frac{d^n h}{dx^n}(x)$$

et l'évaluation en $x = 0$ nous donne :

$$\frac{d^n h}{dx^n}(0) = \frac{d^{n-1}}{dt^{n-1}}(\sigma^n)(0).$$

6. Pour f de classe $\mathcal{C}^{\infty}$ sur $\mathbb{R}$, on a $u = f \circ \varphi$ et pour $(0,t) \in U$:

$$\frac{\partial^n u}{\partial x^n}(0,t) = \frac{d^{n-1}}{dt^{n-1}}\left((\Phi(t))^n f'(t)\right) = \frac{d^{n-1}}{dt^{n-1}}\left((\sigma(t))^n f'(t)\right)$$

donc :

$$\frac{\partial^n u}{\partial x^n}(0,0) = \frac{d^{n-1}}{dt^{n-1}}\left(\sigma^n f'\right)(0)$$

avec $u(x,0) = f \circ h(x)$ et :

$$\frac{\partial^n u}{\partial x^n}(x,0) = \frac{d^n (f \circ h)}{dx^n}(x)$$

et donc :

$$\frac{d^n (f \circ h)}{dx^n}(0) = \frac{d^{n-1}}{dt^{n-1}}\left(\sigma^n f'\right)(0).$$

– IV – Application à la suite (u_n)

1. La fonction τ_p est de classe $\mathcal{C}^\infty$ sur $\mathbb{R} \setminus \{-1\}$ avec :

$$\tau_p'(x) = \frac{1 - px}{(1+x)^{p+2}} > 0$$

pour $x \in \left[0, \frac{1}{p}\right[$, elle est donc continue strictement croissante sur $\left[0, \frac{1}{p}\right]$ et réalise un homéomorphisme de $\left[0, \frac{1}{p}\right]$ sur $\left[0, \frac{p^p}{(p+1)^{p+1}}\right] = [0, \rho_p]$.
Comme elle est $\mathcal{C}^\infty$ de dérivée strictement positive sur $\left[0, \frac{1}{p}\right[$, elle réalise un $\mathcal{C}^\infty$-difféomorphisme de $\left[0, \frac{1}{p}\right[$ sur $[0, \rho_p[$.

2. Prenant $g = \tau_p$ sur $\left]-\frac{1}{p}, \frac{1}{p}\right[$ dans **III.3.** on a $g(0) = 0$, $g'(0) = 1 \neq 0$ et la fonction $\sigma : x \mapsto \frac{x}{g(x)} = (1+x)^{p+1}$ est $\mathcal{C}^\infty$ sur ce voisinage de 0. La formule de réversion de Lagrange s'écrit alors :

$$\frac{d^n h}{dx^n}(0) = w_p^{(n)}(0) = \frac{d^{n-1}}{dt^{n-1}}(\sigma^n)(0)$$

la dérivée d'ordre $n-1$ en 0 du polynôme $\sigma^n(t) = (1+t)^{(p+1)n}$ étant donnée par son développement en série entière :

$$(1+t)^{(p+1)n} = \sum_{k=0}^{(p+1)} \binom{(p+1)n}{k} t^k$$

ce qui donne :

$$w_p^{(n)}(0) = (n-1)! \binom{(p+1)n}{n-1}$$

soit :

$$\frac{w_p^{(n)}(0)}{n!} = \frac{1}{n} \binom{(p+1)n}{n-1}.$$

3. Il s'agit de montrer un théorème de Raabe-Duhamel.
On a :

$$\frac{b_{n+1}}{b_n} = \left(1 + \frac{1}{n}\right)^{-\beta} = 1 - \frac{\beta}{n} + o\left(\frac{1}{n}\right)$$

et :

$$\frac{a_{n+1}}{a_n} - \frac{b_{n+1}}{b_n} = \frac{1}{n}\left(\beta - \alpha + \varepsilon_n\right)$$

où $(\varepsilon_n)_{n\geq 1}$ est une suite réelle qui tend vers 0.
Pour $\alpha > 1$, on choisit β tel que $1 < \beta < \alpha$, de sorte que :

$$\lim_{n\to+\infty} (\beta - \alpha + \varepsilon_n) = \beta - \alpha < 0$$

et il existe un entier n_0 tel que $\beta - \alpha + \varepsilon_n < 0$ pour tout $n \geq n_0$, ce qui donne $\frac{a_{n+1}}{a_n} < \frac{b_{n+1}}{b_n}$ pour tout $n \geq n_0$ et $\sum a_n$ converge comme $\sum b_n$ $(\beta > 1)$.

4. Comme ρ_p est le rayon de convergence de la série entière S_p, cette série converge sur $]-\rho_p, \rho_p[$ et il s'agit d'étudier sa convergence en ρ_p (elle est à coefficients positifs). Notant $a_n = \frac{1}{2n}\binom{n(p+1)}{n-1}$ le coefficient de x^n dans cette série, on a :

$$\begin{aligned}
\frac{a_{n+1}\rho_p^{n+1}}{a_n\rho_p^n} &= \frac{(n(p+1)+(p+1))}{n+1}\prod_{k=1}^{p}\frac{n(p+1)+k}{np+1+k}\frac{p^p}{(p+1)^{p+1}} \\
&= \frac{n+1}{n+1}\prod_{k=1}^{p}\frac{n+\frac{k}{p+1}}{n+\frac{1+k}{p}} \\
&= \prod_{k=1}^{p}\left(1+\frac{k}{(p+1)n}\right)\left(1+\frac{1+k}{pn}\right)^{-1}
\end{aligned}$$

soit :

$$\begin{aligned}
\tfrac{a_{n+1}\rho_p^{n+1}}{a_n\rho_p^n} &= \textstyle\prod_{k=1}^{p}\left(1+\frac{k}{(p+1)n}\right)\prod_{k=1}^{p}\left(1-\frac{k+1}{pn}+o\left(\frac{1}{n}\right)\right) \\
&= \left(1+\frac{\sum\limits_{k=1}^{p} k}{(p+1)n}+o\left(\tfrac{1}{n}\right)\right)\left(1-\frac{\sum\limits_{k=1}^{p}(k+1)}{pn}+o\left(\tfrac{1}{n}\right)\right) \\
&= \left(1+\tfrac{p(p+1)}{2(p+1)n}+o\left(\tfrac{1}{n}\right)\right)\left(1-\tfrac{1}{pn}\left(\tfrac{p(p+1)}{2}+p\right)+o\left(\tfrac{1}{n}\right)\right) \\
&= \left(1+\tfrac{pn}{2}+o\left(\tfrac{1}{n}\right)\right)\left(1-\tfrac{p+3}{2}\tfrac{1}{n}+o\left(\tfrac{1}{n}\right)\right) \\
&= 1+\left(\tfrac{p}{2}-\tfrac{p+3}{2}\right)\tfrac{1}{n}+o\left(\tfrac{1}{n}\right) = 1-\tfrac{3}{2}\tfrac{1}{n}+o\left(\tfrac{1}{n}\right)
\end{aligned}$$

et le théorème de Raabe-Duhamel nous assure la convergence de la série $S_p(\rho_p)$.

5.

(a) Le **IV.2.** nous dit que les fonctions w_p et $2S_p$ ont mêmes développements limités à tous ordres en 0. Il en résulte que les fonctions $2S_p - x(1+2S_p)^{p+1}$ et $x \mapsto w_p - x(1+w_p)^{p+1}$ ont mêmes développements limités à tous ordres en 0.

(b) Pour $x \in [0, \rho_p]$, on a $\tau_p(w_p(x)) = \dfrac{w_p(x)}{(1+w_p(x))^{p+1}} = x$, soit :

$$w_p(x) - x(1+w_p(x))^{p+1} = 0$$

il en résulte que la fonction $2S_p - x(1+2S_p)^{p+1}$, qui est développable en série entière sur $[-\rho_p, \rho_p]$, a toutes ses dérivées en 0 nulles et en conséquence est la fonction nulle sur cet intervalle.

(c) Nous allons montrer que $2S_p$ est l'inverse de τ_p. La fonction S_p est continue strictement croissante sur $[0, \rho_p]$ (sa dérivée est strictement positive sur $]0, \rho_p[$) avec $S_p(0) = 0$ et :

$$2S_p(\rho_p) - \rho_p(1+2S_p(\rho_p))^{p+1} = 0,$$

ce qui donne :

$$\tau_p(2S_p(\rho_p)) = \frac{2S_p(\rho_p)}{(1+2S_p(\rho_p))^{p+1}} = \rho_p$$

et $2S_p(\rho_p) = \dfrac{1}{p}$ puisque $\dfrac{1}{p}$ est l'unique point fixe de ρ_p sur $\mathbb{R}^+$ (étude de $\tau_p(x) - x$). On a donc $2S_p(\rho_p) = \dfrac{1}{p}$. La fonction $2S_p$ est donc croissante de $[0, \rho_p]$ dans $\left[0, \dfrac{1}{p}\right]$ et vérifie $\tau_p(2S_p(x)) = x$ pour tout $x \in [0, \rho_p]$, c'est donc l'inverse de τ_p, soit $2S_p = w_p$.

6.

(a) En **I.8.** on a vu que $\dfrac{1}{2} \leq u_p \leq \dfrac{1}{2} + \dfrac{1}{2p}$, ce qui équivaut à :

$$0 \leq v_p = 2u_p - 1 \leq \frac{1}{p}.$$

(b) L'égalité $\dfrac{v_p}{(1+v_p)^{p+1}} = \dfrac{1}{2^{p+1}}$ (**II.4.a.**) avec $v_p \in \left[0, \dfrac{1}{p}\right]$, s'écrit

$\tau_p(v_p) = \frac{1}{2^{p+1}}$, ce qui équivaut à :

$$\begin{aligned} v_p &= w_p\left(\frac{1}{2^{p+1}}\right) = 2S_p\left(\frac{1}{2^{p+1}}\right) \\ &= \sum_{n=1}^{+\infty} \frac{1}{n}\binom{n(p+1)}{n-1}\frac{1}{2^{(p+1)n}} \end{aligned}$$

et

$$u_p = \frac{1+v_p}{2} = \frac{1}{2} + \sum_{n=1}^{+\infty} \frac{1}{n \cdot 2^{n(p+1)+1}}\binom{n(p+1)}{n-1}.$$

Deuxième partie

ALGEBRE & GEOMETRIE

Chapitre 5

CAPES externe 2006, épreuve 2

5.1 Énoncé

Définitions et notations

On considère un espace affine euclidien orienté $\mathcal{E}$ de dimension 3, de direction E, muni d'un repère orthonormal direct $\mathcal{R}_0 = (O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$.
Le sous-espace affine de $\mathcal{E}$ d'équation $(z = 0)$ sera noté $\mathcal{P}$, et sa direction P.
Par abus d'écriture, à partir de la partie III, le repère $(O, \overrightarrow{i}, \overrightarrow{j})$ de $\mathcal{P}$ sera également noté $\mathcal{R}_0$.
Si $\mathcal{R}$ est un repère d'un espace affine $\mathcal{X}$ de dimension quelconque n et si M est un point de $\mathcal{X}$, nous noterons $M(x_1, ..., x_n)_{\mathcal{R}}$ pour signifier que x_1, ..., x_n sont les coordonnées de M dans le repère $\mathcal{R}$.

La partie de $\mathcal{P}$ formée des points à coordonnées entières est notée $\mathcal{Z}$:

$$M(x, y)_{\mathcal{R}_0} \in \mathcal{Z} \text{ si et seulement si } (x, y) \in \mathbb{Z}^2.$$

Si A et B sont deux points de $\mathcal{E}$, nous noterons AB la distance de A à B, (AB) la droite passant par les points A et B (quand $A \neq B$) et $[A, B]$ le segment d'extrémités A et B.
On note $\mathcal{Q}$ la quadrique de $\mathcal{E}$ d'équation :

$$(\mathcal{Q}) \qquad x^2 - 3xy + y^2 + x - y - \frac{1}{2}z^2 + \frac{\sqrt{10}}{5}z = 0$$

et $\mathcal{C}$ la conique intersection de $\mathcal{Q}$ et du plan $\mathcal{P}$:

$$(\mathcal{C}) \qquad \begin{cases} x^2 - 3xy + y^2 + x - y = 0 \\ z = 0. \end{cases}$$

On note GA $(\mathcal{P})$ le groupe affine de $\mathcal{P}$, c'est-à-dire l'ensemble des bijections affines de $\mathcal{P}$ sur lui-même : GA $(\mathcal{P})$ est un groupe pour la composition. On note $\mathcal{M}_2(\mathbb{R})$ l'algèbre des matrices réelles carrées d'ordre 2. Le sous-groupe multiplicatif des éléments inversibles de cette algèbre est noté $\mathrm{GL}_2(\mathbb{R})$.

Le but de ce problème est d'étudier l'équation diophantienne :

$$(\Sigma) \qquad n^2 - 3np + p^2 + n - p = 0,$$

c'est-à-dire de déterminer l'ensemble $\mathcal{S}$ des points de $\mathcal{C}$ à coordonnées entières : $\mathcal{S} = \mathcal{C} \cap \mathcal{Z}$.

La partie I présente une étude géométrique de la quadrique $\mathcal{Q}$ et de la conique $\mathcal{C}$; la partie II donne quelques méthodes arithmétiques d'étude de (Σ) ; la partie III introduit une famille de transformations affines qui permet, dans la partie IV, de décrire l'ensemble $\mathcal{S}$.

Les parties I et II sont indépendantes et la partie III est très largement indépendante des deux parties précédentes.

Partie I : Etude de la quadrique $\mathcal{Q}$ et de la conique $\mathcal{C}$

I.1. Intersections de Q avec une famille de plans

On pose $\overrightarrow{u} = \dfrac{\sqrt{2}}{2}(\overrightarrow{i} + \overrightarrow{j})$ et $\overrightarrow{v} = \overrightarrow{k}$.

a) Déterminer le vecteur $\overrightarrow{w}$ tel que $(\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ soit une base orthonormale directe de E.

b) On pose $\mathcal{R}_1 = (O, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$. Soit M un point de $\mathcal{E}$; on le représente dans les deux repères par $M = M(x, y, z)_{\mathcal{R}_0} = M(x_1, y_1, z_1)_{\mathcal{R}_1}$. Exprimer x, y et z en fonction de x_1, y_1 et z_1, puis en déduire l'équation de $\mathcal{Q}$ dans le repère $\mathcal{R}_1$.

c) Pour $t \in \mathbb{R}$, soit $\mathcal{P}_t$ le plan d'équation $z_1 = t$ relativement au repère $\mathcal{R}_1$. Préciser la position de $\mathcal{P}_t$ dans $\mathcal{R}_0$ et en faire un croquis. Montrer que l'intersection de $\mathcal{P}_t$ et de $\mathcal{Q}$ est un cercle dont on précisera le centre C_t et le rayon R_t.

d) Préciser la valeur de t pour laquelle le cercle précédent se réduit à un point. Soit S ce point ; vérifier que

$$S = \left(-\frac{1}{5}, \frac{1}{5}, \frac{\sqrt{10}}{5}\right)_{\mathcal{R}_0}.$$

I.2. Nature de $\mathcal{Q}$ et de $\mathcal{C}$

Soit $\mathcal{R}$ le repère $(S, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$; on note (X, Y, Z) les coordonnées d'un point de $\mathcal{E}$ dans ce nouveau repère. On note $\mathcal{P}'$ le plan admettant $\mathcal{R}' = (S, \overrightarrow{v}, \overrightarrow{w})$

pour repère orthonormal.

a) Montrer que l'équation de $\mathcal{Q}$ dans le repère $\mathcal{R}$ est $X^2 + Y^2 = 5Z^2$.

b) Quelle est la nature de $\mathcal{Q}$? On remarquera en particulier que $\mathcal{Q}$ est une surface de révolution et on précisera son axe.

c) Montrer qu'un point $M\,(X, Y, Z)_{\mathcal{R}}$ est élément de $\mathcal{P}$ si et seulement si $Y = -\dfrac{\sqrt{10}}{5}$.

Faire une figure, sur une feuille de papier millimétrée, représentant, dans le repère $\mathcal{R}'$, la droite d'intersection $\mathcal{D} = \mathcal{P} \cap \mathcal{P}'$, ainsi que les deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ formant $\mathcal{Q} \cap \mathcal{P}'$. On prendra une unité égale à 8 cm.

Pour toute la fin de cette partie, cette figure sera un outil important. On y placera, les éléments définis ci-dessous ou leurs projections sur $\mathcal{P}'$ au fur et à mesure qu'ils apparaîtront utiles.

Quelle est la nature de la conique $\mathcal{C}$?

d) Montrer qu'il existe deux cercles dans $\mathcal{P}'$, de même rayon et centrés sur l'axe $(S, \overrightarrow{w})$, tangents aux trois droites $\mathcal{D}$, $\mathcal{D}_1$ et $\mathcal{D}_2$. On note Ω_1 et Ω_2 leurs centres respectifs, et on note ρ la valeur commune de leurs rayons.

e) On note $\mathcal{S}_1$ et $\mathcal{S}_2$ les sphères de centres respectifs Ω_1 et Ω_2, et de rayon ρ. Montrer que ces sphères sont tangentes au plan $\mathcal{P}$ en deux points notés F_1 et F_2, et tangentes à $\mathcal{Q}$ le long de deux cercles que l'on note $\mathcal{C}_1$ et $\mathcal{C}_2$. Représenter sur la figure précédente les projections orthogonales sur $\mathcal{P}'$ de ces deux cercles, ainsi que les points F_1 et F_2.

I.3. Deux caractérisations de $\mathcal{C}$

a) Soit M un point quelconque de l'intersection $\mathcal{C} = \mathcal{Q} \cap \mathcal{P}$. Montrer que la droite (MS) est contenue dans $\mathcal{Q}$. On nomme T_1 et T_2 les intersections respectives de (MS) et des cercles $\mathcal{C}_1$ et $\mathcal{C}_2$. Montrer que $MT_1 = MF_1$ et $MT_2 = MF_2$. Montrer par ailleurs que $|MT_1 - MT_2|$ est constant lorsque M décrit $\mathcal{C}$. Quelle propriété de $\mathcal{C}$ peut-on retrouver ainsi ?

b) Pour $i \in \{1, 2\}$, on nomme Δ_i la droite d'intersection du plan $\mathcal{P}$ et du plan contenant le cercle $\mathcal{C}_i$, et U_i le centre de $\mathcal{C}_i$. Pour M point quelconque de l'intersection $\mathcal{C} = \mathcal{Q} \cap \mathcal{P}$, soit H_i la projection orthogonale de M sur Δ_i. Vérifier que les points M, S, H_i, T_i et U_i sont coplanaires. En étudiant la figure formée par ces cinq points, prouver que le rapport MH_i/MT_i reste constant quand M décrit $\mathcal{C}$. Quelle propriété de $\mathcal{C}$ peut-on retrouver ainsi ?

Partie II : Résolution de l'équation diophantienne pour de petites valeurs de n

Pour n et p deux entiers tels que $0 \leq p \leq n$, on note $\binom{n}{p}$ le coefficient binomial :

$$\binom{n}{p} = \frac{n!}{p!(n-p)!}$$

avec la convention $0! = 1$. Pour n et p entiers naturels supérieurs ou égaux à 1, on s'intéresse, lorsqu'elle a un sens, à l'équation :

$$(\Sigma_1) \qquad \binom{n}{p-1} = \binom{n-1}{p}.$$

II.1. Une étude élémentaire

a) Montrer que cette équation est équivalente au système :

$$\begin{cases} 2 \leq p+1 \leq n \\ n^2 + p^2 - 3np + n - p = 0. \end{cases}$$

b) Pour n entier supérieur ou égal à 1, montrer que le polynôme de variable X : $n^2 - 3nX + X^2 + n - X$ possède deux racines réelles, que l'on écrira sous la forme $X_1 = \frac{a_n - \sqrt{b_n}}{2}$ et $X_2 = \frac{a_n + \sqrt{b_n}}{2}$ où a_n et b_n sont deux entiers naturels. Pour quelles valeurs de n a-t-on $2 \leq X_1 + 1 \leq n$? Et pour quelles valeurs de n a-t-on $2 \leq X_2 + 1 \leq n$?

c) Montrer que si b est un entier naturel, $\sqrt{b}$ est rationnel si et seulement si b est un carré parfait.

d) On suppose que (n, p) est une solution de (Σ_1). Montrer que $2 \leq n$, que $5n^2 + 2n + 1$ est un carré parfait et donner une expression de p en fonction de n.

e) Réciproquement, soit n un entier naturel supérieur ou égal à 2 tel que $5n^2 + 2n + 1$ soit un carré parfait. Montrer qu'il existe un unique p tel que (n, p) soit solution de (Σ_1).

f) Pour n_0 entier naturel non nul, comment peut-on calculer tous les couples (n, p) solutions de (Σ_1) avec $1 \leq n \leq n_0$? On pourra donner un algorithme de calcul de ces solutions, sans utiliser un langage de programmation précis.

II.2 Une méthode plus arithmétique

Soit (n, p) une solution de (Σ_1).

a) On suppose que n et p sont premiers entre eux. Montrer que

$$np = (n-p)(n-p+1)$$

et en déduire que n divise $p - 1$. Quelles sont toutes les solutions de (Σ_1) formées d'entiers premiers entre eux ?

b) On ne suppose plus maintenant que n et p sont premiers entre eux : on note $r = n \wedge p$ leur plus grand commun diviseur commun et on pose $n = ru$ et $p = rv$. Montrer successivement :

• r divise $u - v$; • $r = u - v$; • $v = \dfrac{\sqrt{5r^2+4} - r}{2}$; • $r^2 < \dfrac{2p}{\sqrt{5} - 1}$.

c) Faire la liste de tous les couples (n, p) solutions de (Σ_1) pour $n \leq 105$.

Partie III : Un groupe de transformations affines conservant $\mathcal{S}$

Dans cette partie et la suivante, nous travaillons exclusivement dans le plan $\mathcal{P}$, dont le repère $(O, \overrightarrow{i}, \overrightarrow{j})$ est encore noté $\mathcal{R}_0$. Les vecteurs $\overrightarrow{u}$ et $\overrightarrow{v}$ et le repère $\mathcal{R}_1$ définis ci-dessous n'ont pas de rapport avec les éléments de mêmes noms définis dans la partie I.

III.1. Définition d'un nouveau repère $\mathcal{R}_1$ associé à la conique $\mathcal{C}$

a) Soit $I(-1/5, 1/5)_{\mathcal{R}_0}$. On pose alors $x_1 = x + 1/5$ et $y_1 = y - 1/5$. Quelle est l'équation de $\mathcal{C}$ dans le repère $(I, \overrightarrow{i}, \overrightarrow{j})$?

b) Mettre la forme quadratique $a^2 + b^2 - 3ab$ sous la forme d'un produit de formes linéaires. On pourra considérer $a^2 + b^2 - 3ab$ comme un trinôme d'inconnue b.

c) En déduire qu'il existe une base $(\overrightarrow{u}, \overrightarrow{v})$ de P telle que :

• les relations entre les coordonnées (x, y) dans le repère $\mathcal{R}_0$ et les coordonnées (X, Y) dans le repère $\mathcal{R}_1 = (I, \overrightarrow{u}, \overrightarrow{v})$ soient de la forme :

$$\begin{cases} X = \alpha\left(x + \dfrac{1}{5}\right) - \left(y - \dfrac{1}{5}\right) \\ Y = \beta\left(x + \dfrac{1}{5}\right) + \left(y - \dfrac{1}{5}\right) \end{cases}$$

avec $\alpha + \beta > 0$;

• l'équation de $\mathcal{C}$ dans le repère $(I, \overrightarrow{u}, \overrightarrow{v})$ s'écrive : $5XY + 1 = 0$.

Expliciter les valeurs de α et β, ainsi que les relations exprimant les anciennes coordonnées (x, y) en fonction des nouvelles coordonnées (X, Y).

d) Que sont les axes du nouveau repère $\mathcal{R}_1$ pour la conique $\mathcal{C}$?

III. 2. Transformations affines conservant $\mathcal{C}$

Nous étudions dans ce paragraphe l'ensemble G_1 des éléments de $\mathrm{GA}(\mathcal{P})$ qui conservent la conique $\mathcal{C}$:

$$G_1 = \{h \in \mathrm{GA}(\mathcal{P}) \;/\; h(\mathcal{C}) = \mathcal{C}\}.$$

a) Montrer qu'un élément h de $\mathrm{GA}(\mathcal{P})$ est élément de G_1 si et seulement si $h(\mathcal{C}) \subset \mathcal{C}$.

b) Montrer que G_1 est un sous-groupe de $\mathrm{GA}(\mathcal{P})$.

c) Soit $h \in \mathrm{GA}(\mathcal{P})$. Montrer qu'il existe un et un seul sextuplet (a, b, c, d, e, f) de réels tel que, pour tout point $M(X, Y)_{\mathcal{R}_1}$, l'image $M' = h(M)$ de M par h ait pour coordonnées, toujours dans le repère $\mathcal{R}_1$, $X' = aX + bY + c$ et $Y' = dX + eY + f$. Justifier que $ae - bd \neq 0$.

d) Montrer que si h est élément de G_1, le sextuplet (a, b, c, d, e, f) qui lui est associé vérifie les relations :

$$\begin{cases} ad = af + cd = bf + ce = be = 0 \\ 5cf - ae - bd = -1 \\ ae - bd \neq 0. \end{cases}$$

e) En déduire que le groupe G_1 est formé des transformations de la forme $M(X, Y)_{\mathcal{R}_1} \mapsto M'(\mu X, Y/\mu)_{\mathcal{R}_1}$ et $M(X, Y)_{\mathcal{R}_1} \mapsto M'(\mu Y, X/\mu)_{\mathcal{R}_1}$ où μ décrit $\mathbb{R}\backslash\{0\}$. Parmi ces transformations, lesquelles sont des symétries ?

f) On note G_1' la partie de $\mathrm{GL}_2(\mathbb{R})$ définie par :

$$A \in G_1' \iff \exists \mu \in \mathbb{R}^* \quad A = \begin{pmatrix} \mu & 0 \\ 0 & 1/\mu \end{pmatrix} \quad \text{ou} \quad A = \begin{pmatrix} 0 & \mu \\ 1/\mu & 0 \end{pmatrix}.$$

Montrer que G_1' est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$ pour le produit matriciel et que l'application qui à toute matrice $\begin{pmatrix} a & b \\ d & e \end{pmatrix}$ de G_1' associe la transformation affine $M(X, Y)_{\mathcal{R}_1} \mapsto M'(aX + bY, dX + eY)_{\mathcal{R}_1}$ est un isomorphisme de G_1' sur G_1.

III. 3. Transformations affines conservant $\mathcal{Z}$

Nous nous intéressons dans ce paragraphe à l'ensemble G_2 des éléments de $\mathrm{GA}(\mathcal{P})$ qui conservent les points à coordonnées entières :

$$G_2 = \{h \in \mathrm{GA}(\mathcal{P}) \;/\; h(\mathcal{Z}) = \mathcal{Z}\}.$$

a) Un élément quelconque $h \in \mathrm{GA}(\mathcal{P})$ vérifiant $h(\mathcal{Z}) \subset \mathcal{Z}$ est-il nécessairement élément de G_2 ?

b) Montrer que G_2 est un sous-groupe de $\mathrm{GA}(\mathcal{P})$.

c) Montrer que les éléments de G_2 sont exactement les applications de la forme

$$M(x, y)_{\mathcal{R}_0} \mapsto M'(ax + by + c, dx + ey + f)_{\mathcal{R}_0}$$

où $(a, b, c, d, e, f) \in \mathbb{Z}^6$ avec $|ae - bd| = 1$.

III. 4. Le groupe Γ

a) Montrer qu'il existe deux points P_1 et P_2 tels que :

- $P_1 \neq O$, $P_2 \neq O$ et $P_1, P_2 \in \mathcal{S}$;
- P_1 est d'ordonnée nulle et P_2 est d'abscisse nulle.

Montrer qu'il existe deux transformations affines f_1 et f_2 telles que :

- $f_1(I) = I$, $f_1(O) = P_1$ et $f_1(P_1) = O$;
- $f_2(I) = I$, $f_2(O) = P_2$ et $f_2(P_2) = O$.

Si M est un point quelconque de $\mathcal{P}$, nous noterons respectivement (x, y) et (X, Y) les coordonnées de M dans les repères $\mathcal{R}_0$ et $\mathcal{R}_1$. De même, pour $i = 1$ et 2, nous noterons (x_i, y_i) et (X_i, Y_i) les coordonnées de $f_i(M)$ dans les repères $\mathcal{R}_0$ et $\mathcal{R}_1$. Nous avons donc :

$$\begin{aligned} M(x,y)_{\mathcal{R}_0} &= M(X,Y)_{\mathcal{R}_1} \\ f_1(M)(x_1,y_1)_{\mathcal{R}_0} &= f_1(M)(X_1,Y_1)_{\mathcal{R}_1} \\ f_2(M)(x_2,y_2)_{\mathcal{R}_0} &= f_2(M)(X_2,Y_2)_{\mathcal{R}_1} \end{aligned}$$

Exprimer x_1, y_1, x_2 et y_2 en fonction de x et y et démontrer les relations matricielles :

$$\begin{pmatrix} X_1 \\ Y_1 \end{pmatrix} = \begin{pmatrix} 0 & \lambda \\ \dfrac{1}{\lambda} & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} X_2 \\ Y_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

où $\lambda = \dfrac{7 + 3\sqrt{5}}{2}$. En déduire que f_1 et f_2 sont toutes deux des symétries appartenant à $G_1 \cap G_2$.

b) On s'intéresse maintenant au sous-groupe Γ de $\mathrm{GA}(\mathcal{P})$ engendré par f_1 et f_2. Montrer que les éléments de Γ sont les éléments h de $\mathrm{GA}(\mathcal{P})$ qui s'écrivent sous l'une des formes suivantes :

(i) $h = (f_1 \circ f_2)^k$ avec $k \in \mathbb{Z}$;

(ii) $h = f_2 \circ (f_1 \circ f_2)^k$ avec $k \in \mathbb{Z}$.

c) Montrer que Γ est isomorphe au sous-groupe Γ_1 de $\mathrm{GL}_2(\mathbb{R})$ engendré par les matrices A_1 et A_2 :

$$A_1 = \begin{pmatrix} 0 & \lambda \\ \dfrac{1}{\lambda} & 0 \end{pmatrix} \qquad A_2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

Calculer $A_1 A_2$ et en déduire :

$$\Gamma_1 = \left\{ \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix} / \, k \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} 0 & \lambda^{-k} \\ \lambda^k & 0 \end{pmatrix} / \, k \in \mathbb{Z} \right\}.$$

En déduire que la décomposition obtenue au b) est unique, c'est-à-dire que chaque élément h de Γ correspond à un et un seul des deux cas (i) ou (ii) et que l'entier relatif k intervenant dans la décomposition de h est unique.

d) Soit H un groupe dont la loi est notée mutiplicativement : l'élément neutre de H sera donc noté 1. On suppose qu'il existe deux éléments a_1 et a_2 de H tels que $a_1^2 = a_2^2 = 1$. Montrer qu'il existe un unique morphisme de groupe $\phi : \Gamma \to H$ tel que $\phi(f_1) = a_1$ et $\phi(f_2) = a_2$.

III. 5. Utilisation de Γ pour engendrer une infinité de points de $\mathcal{S}$

a) Montrer que $\mathcal{S}$ est stable par Γ, c'est-à-dire que pour tout élément h de Γ et pour tout élément M de $\mathcal{S}$, $h(M)$ est élément de $\mathcal{S}$.
Comme l'origine O de $\mathcal{R}_0$ est élément de $\mathcal{S}$, on en déduit donc que les points M_k et N_k définis pour $k \in \mathbb{Z}$ par :

$$\begin{cases} M_k = (f_1 \circ f_2)^k (O) \\ N_k = f_2 \circ (f_1 \circ f_2)^k (O) = f_2 (M_k) \end{cases}$$

sont tous éléments de $\mathcal{S}$. Calculer M_1, M_2 et M_3 et comparer avec les résultats obtenus à la partie II.

b) Donner l'expression des coordonnées (x_k, y_k) de M_k dans le repère $\mathcal{R}_0$, en fonction de k et λ. Quelle transformation permet-elle d'obtenir M_{-k} à partir de M_k ?

c) Montrer que les applications :

$$\begin{cases} \phi_1 : x \longmapsto \dfrac{1}{2}\left(1 + 3x - \sqrt{1 + 2x + 5x^2}\right) \\ \phi_2 : x \longmapsto \dfrac{1}{2}\left(1 + 3x + \sqrt{1 + 2x + 5x^2}\right) \end{cases}$$

sont des bijections de $\mathbb{R}$ sur lui-même. Quelles sont leurs applications réciproques ?

On note $\mathcal{C}_1$ et $\mathcal{C}_2$ les parties de $\mathcal{P}$ définies par :

$$\begin{cases} M(x,y)_{\mathcal{R}_0} \in \mathcal{C}_1 \iff y = \phi_1(x), \\ M(x,y)_{\mathcal{R}_0} \in \mathcal{C}_2 \iff y = \phi_2(x). \end{cases}$$

Montrer que $\mathcal{C}_1$ et $\mathcal{C}_2$ forment une partition de $\mathcal{C}$. Représenter, rapidement les parties $\mathcal{C}_1$ et $\mathcal{C}_2$, ainsi que les points M_{-1}, M_0, M_1, M_2, N_{-1}, N_0 et N_1.

d) Montrer que les applications f_1 et f_2 échangent les courbes $\mathcal{C}_1$ et $\mathcal{C}_2$, et donc que $\mathcal{C}_1$ et $\mathcal{C}_2$ sont globalement invariantes par $f_1 \circ f_2$. Sur quelles parties de $\mathcal{C}$ les points M_k et N_k sont-ils situés ?

Partie IV : Résolution de (Σ)

Soit $P\,(n,p)_{\mathcal{R}_0}$ un point de $\mathcal{S}$ distinct de O. Le but de cette partie est de démontrer que P est image de O par un élément h de Γ, c'est-à-dire qu'il existe $k \in \mathbb{Z}$ tel que $P = M_k$ ou $P = N_k$.

IV. 1. Premier cas : P est élément de $\mathcal{C}_1$ et $n > 0$

Soit la suite $(P_i)_{i\geq 0}$ définie par récurrence :

$$\begin{cases} P_0 = P \\ P_{i+1} = (f_1 \circ f_2)^{-1}(P_i) \text{ pour tout } i \geq 0. \end{cases}$$

Pour tout i, on notera α_i et β_i les coordonnées de P_i dans le repère $\mathcal{R}_0$.

a) Montrer que l'on a, pour tout i de $\mathbb{N}$, $\alpha_{i+1} = \phi_2^{-1} \circ \phi_1(\alpha_i)$ et $\beta_i = \phi_1(\alpha_i)$.

b) Montrer que la suite $(\alpha_i)_{i\geq 0}$ est strictement décroissante et non minorée. En déduire qu'il existe un entier $k \geq 1$ tel que $\alpha_k \leq 0 < \alpha_{k-1}$.

c) Montrer que $\alpha_k = 0$ puis que $P = M_k$.

d) Quel est l'ensemble des solutions de l'équation (Σ_1) ?

IV. 2. Deuxième cas : P est élément de $\mathcal{C}_1$ et $n < 0$

a) Montrer que le point $P'\,(-p,-n)_{\mathcal{R}_0}$ est élément de $\mathcal{C}_1$.

b) En déduire qu'il existe un entier relatif k strictement négatif tel que $P = M_k$.

IV. 3. Troisième cas : P est élément de $\mathcal{C}_2$

Montrer qu'il existe k élément de $\mathbb{Z}$ tel que $P = N_k$.

5.2 Corrigé

I.1.a. En notant $\wedge$ le produit vectoriel et en identifiant chaque vecteur de E avec ses coordonnées dans la base $(\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$, on obtient

$$\overrightarrow{u} \wedge \overrightarrow{v} = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} \\ 0 \end{pmatrix} \wedge \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} \\ -\frac{\sqrt{2}}{2} \\ 0 \end{pmatrix}.$$

I.1.b. ► La matrice de passage de la base $(\overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k})$ vers la base $(\overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ est

$$P = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \end{pmatrix}.$$

Elle nous permet d'exprimer les anciennes coordonnées de M en fonction des nouvelles :

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} x_1 \\ y_1 \\ z_1 \end{pmatrix}$$

soit

$$\begin{cases} x = \frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}}{2}z_1 \\ y = \frac{\sqrt{2}}{2}x_1 - \frac{\sqrt{2}}{2}z_1 \\ z = y_1. \end{cases}$$

► On a

$$x^2 + y^2 = \left(\frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}}{2}z_1\right)^2 + \left(\frac{\sqrt{2}}{2}x_1 - \frac{\sqrt{2}}{2}z_1\right)^2 = x_1^2 + z_1^2,$$

et

$$3xy = 3\left(\frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}}{2}z_1\right)\left(\frac{\sqrt{2}}{2}x_1 - \frac{\sqrt{2}}{2}z_1\right) = \frac{3}{2}x_1^2 - \frac{3}{2}z_1^2.$$

Une équation de $\mathcal{Q}$ dans le repère $\mathcal{R}_1$ sera donc

$$x_1^2+z_1^2-\frac{3}{2}x_1^2+\frac{3}{2}z_1^2+\left(\frac{\sqrt{2}}{2}x_1 + \frac{\sqrt{2}}{2}z_1\right)-\left(\frac{\sqrt{2}}{2}x_1 - \frac{\sqrt{2}}{2}z_1\right)-\frac{1}{2}y_1^2+\frac{\sqrt{10}}{5}y_1 = 0$$

ou encore

$$\mathcal{Q} : \quad \frac{1}{2}x_1^2 - \frac{5}{2}z_1^2 + \frac{1}{2}y_1^2 - \frac{\sqrt{10}}{5}y_1 - \sqrt{2}z_1 = 0.$$

I.1.c. Le plan $\mathcal{P}_t : z_1 = t$ est parallèle au plan de coordonnées $(O, \overrightarrow{u}, \overrightarrow{v})$. C'est donc un plan orthogonal à $\overrightarrow{w}$. Sur la FIG. 5.1, on a donc tracé le vecteur $\overrightarrow{w} = \frac{\sqrt{2}}{2}\overrightarrow{i} - \frac{\sqrt{2}}{2}\overrightarrow{j}$, puis dessiné un plan orthogonal à ce vecteur. Un système d'équations cartésiennes de $\mathcal{P}_t \cap \mathcal{Q}$ est

$$\begin{cases} \frac{1}{2}x_1^2 + \frac{1}{2}y_1^2 - \frac{\sqrt{10}}{5}y_1 = \frac{5}{2}t^2 + \sqrt{2}t \\ z_1 = t \end{cases}$$

La première équation de ce système s'écrivant

$$\frac{1}{2}x_1^2 + \frac{1}{2}\left(y_1 - \frac{\sqrt{10}}{5}\right)^2 = \frac{5}{2}t^2 + \sqrt{2}t + \frac{1}{5}$$

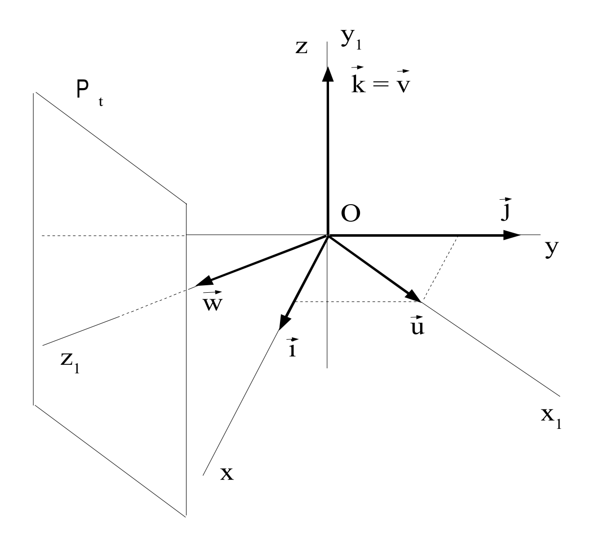


FIG. 5.1 – Représentation de $\mathcal{P}_t$

ou encore

$$x_1^2 + \left(y_1 - \frac{\sqrt{10}}{5}\right)^2 = 5\left(t + \frac{\sqrt{2}}{5}\right)^2,$$

on reconnaît une équation du cercle de centre $C_t = (0, \frac{\sqrt{10}}{5}, t)_{\mathcal{R}_1}$ et de rayon $R_t = \left|t + \frac{\sqrt{2}}{5}\right| \sqrt{5}$.

Remarque : Je m'autorise parfois à identifier "points" et "système de coordonnées de ce point dans un repère donné", donc à écrire $C_t = (0, \frac{\sqrt{10}}{5}, t)_{\mathcal{R}_1}$.

I.1.d. Le cercle est réduit à un point quand $t = -\frac{\sqrt{2}}{5}$, et l'on trouve alors

$$S = (0, \frac{\sqrt{10}}{5}, -\frac{\sqrt{2}}{5})_{\mathcal{R}_1}.$$

Les coordonnées de S dans $\mathcal{R}$ seront donc

$$\begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{2}}{2} & 0 & \frac{\sqrt{2}}{2} \\ \frac{\sqrt{2}}{2} & 0 & -\frac{\sqrt{2}}{2} \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 \\ \frac{\sqrt{10}}{5} \\ -\frac{\sqrt{2}}{5} \end{pmatrix} = \begin{pmatrix} -\frac{1}{5} \\ \frac{1}{5} \\ \frac{\sqrt{10}}{5} \end{pmatrix},$$

comme prévu.

Remarques : α) Les formules de changement de bases ou de repères affines sont à retenir parfaitement car rendent de bons services "à certains moments" (réviser ces formules par ex. en [15], § 1.6.1). La première partie de ce problème nous offre l'occasion de les employer.

β) Les vecteurs-colonnes de P forment une base orthonormale directe, de sorte que P soit une matrice orthogonale positive. C'est donc la matrice d'une rotation vectorielle, et nous pouvons affirmer que le nouveau repère se déduit de l'ancien par une rotation d'axe à déterminer. Cette remarque pourrait être utile dans la suite, et c'est en tout cas ainsi que l'on peut réagir en abordant les premières questions du problème.
Toutes les généralités concernant les applications orthogonales (listées en [15], § 7.1) sont à connaître par coeur. La classification des isométries de l'espace (donnée par exemple en [15], § 7.4) est aussi à savoir... sur le bout des doigts. Si le lecteur prépare un concours en s'entraînant sur des annales, c'est le moment pour lui de réviser tout le cours sur les applications orthogonales.

I.2.a. Les formules de changement de repère de $\mathcal{R}_1 = (O, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ vers $\mathcal{R} = (S, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$ sont

$$\begin{cases} x_1 = X \\ y_1 = Y + \frac{\sqrt{10}}{5} \\ z_1 = Z - \frac{\sqrt{2}}{5}. \end{cases}$$

En remplaçant dans l'équation de $\mathcal{Q}$ dans $\mathcal{R}_1$ obtenue en I.1.b, on trouve

$$\frac{1}{2}X^2 - \frac{5}{2}\left(Z - \frac{\sqrt{2}}{5}\right)^2 + \frac{1}{2}\left(Y + \frac{\sqrt{10}}{5}\right)^2 - \frac{\sqrt{10}}{5}\left(Y + \frac{\sqrt{10}}{5}\right) - \sqrt{2}\left(Z - \frac{\sqrt{2}}{5}\right) = 0,$$

et après réduction, $\mathcal{Q} : X^2 + Y^2 = 5Z^2$.

I.2.b. L'équation $X^2 + Y^2 - 5Z^2 = 0$ de $\mathcal{Q}$ dans $\mathcal{R}_1$ est exceptionnelle : dans son premier membre, elle fait intervenir un polynôme homogène de degré 2. On peut tout de suite affirmer que $\mathcal{Q}$ est un cône d'axe l'axe des Z, autrement dit la droite Δ passant par S et de vecteur directeur $\overrightarrow{w}$ (que nous noterons indifféremment $\Delta = S + \mathbb{R}\overrightarrow{w}$ ou $\Delta = (S, \overrightarrow{w})$.
Comme il existe un plan orthogonal à Δ interceptant $\mathcal{Q}$ suivant un cercle (la question I.1.c nous montre que tous les plans orthogonaux à Δ conviennent, excepté celui passant par S), on peut affirmer que $\mathcal{Q}$ est un cône de révolution d'axe Δ.

Remarque : Il existe d'autres façons de répondre à cette question. On peut par exemple remarquer que la question I.1.c nous permet d'écrire $\mathcal{Q}$ comme la

réunion disjointe de tous les cercles $\mathcal{C}_t$ lorsque t décrit $\mathbb{R}$, soit

$$\mathcal{Q} = \bigsqcup_{t\in\mathbb{R}} \mathcal{C}_t.$$

Comme tous ces cercles sont dessinés dans des plans orthogonaux à Δ et centrés sur Δ, cela suffit pour que l'on puisse affirmer que $\mathcal{Q}$ est un cône de révolution d'axe Δ.

I.2.c. Le plan $\mathcal{P}$ a pour équation $z = 0$ dans $\mathcal{R}_0$. Comme $z = y_1 = Y + \frac{\sqrt{10}}{5}$, $\mathcal{P}$ admettra l'équation $Y = -\frac{\sqrt{10}}{5}$ dans $\mathcal{R}$. Rappelons les notations (en nous permettant de petits abus d'écriture bien commodes) :

$$\begin{array}{lll} \mathcal{R}_0 = (O, \overrightarrow{i}, \overrightarrow{j}, \overrightarrow{k}) \ ; & \mathcal{R}_1 = (O, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w}) \ ; & \mathcal{R} = (S, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w}) \ ; \\ \mathcal{P} = (O, \overrightarrow{i}, \overrightarrow{j}) \ ; & \mathcal{P}' = \mathcal{R}' = (S, \overrightarrow{v}, \overrightarrow{w}). & \end{array}$$

On a

$$\mathcal{D} = \mathcal{P} \cap \mathcal{P}' = \left\{ (X,Y,Z)_{\mathcal{R}} \,/\, Y = -\frac{\sqrt{10}}{5} \text{ et } X = 0 \right\}$$

et

$$\begin{aligned} \mathcal{Q} \cap \mathcal{P}' &= \left\{ (X,Y,Z)_{\mathcal{R}} \,/\, X^2 + Y^2 = 5Z^2 \text{ et } X = 0 \right\} \\ &= \left\{ (X,Y,Z)_{\mathcal{R}} \,/\, Z = \pm\frac{1}{\sqrt{5}} Y \right\}. \end{aligned}$$

Sur la FIG. 5.2, $\mathcal{Q} \cap \mathcal{P}$ apparaît bien comme la réunion de deux droites $\mathcal{D}_1$ et $\mathcal{D}_2$ d'équations $Z = \pm\frac{1}{\sqrt{5}}Y$. On connaît des équations de $\mathcal{Q}$ et $\mathcal{P}$ dans le repère $\mathcal{R}$:

$$\mathcal{Q} : \quad X^2 + Y^2 = 5Z^2 \quad \text{et} \quad \mathcal{P} : \quad Y = -\frac{\sqrt{10}}{5},$$

de sorte que $\mathcal{C}$ admette l'équation $5Z^2 - X^2 = 2/5$. On reconnaît l'équation d'une hyperbole d'axes X et Z (Z étant l'axe transverse : on reconnaît la droite $\mathcal{D}$).

Remarque : La conique $\mathcal{C}$ est l'intersection d'un cône de révolution $\mathcal{Q}$ et d'un plan $\mathcal{P}$ tel que l'axe de $\mathcal{Q}$ soit faiblement parallèle à $\mathcal{P}$. Cela suffit pour que l'on puisse affirmer que $\mathcal{C}$ est une hyperbole, mais on utilise alors une partie du cours sur les coniques qui constitue "un approfondissement" et ne fait pas partie du bagage standard du candidat. Il s'agit du Théorème de Dandelin et Quételet.
Le lecteur intéressé pourra, s'il le désire, se référer à la Section 22.2 de [15] sur les Théorèmes belges, théorèmes qui se trouvent être au coeur de nos préoccupations jusqu'à la fin de la partie I !

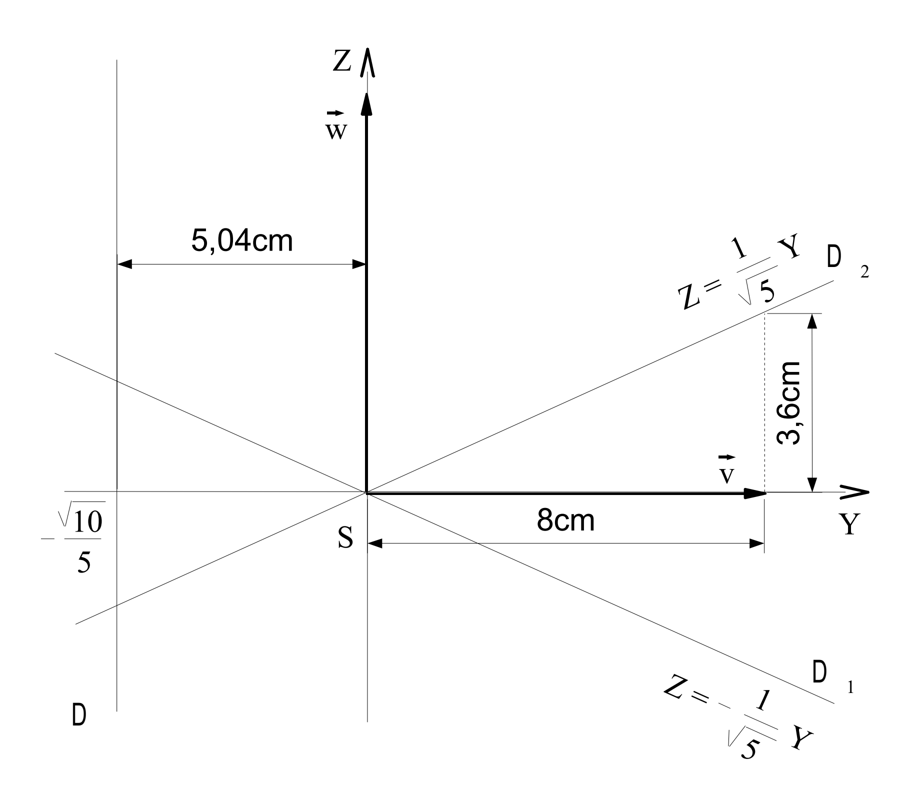


FIG. 5.2 – Figure dans le plan $\mathcal{P}'$

I.2.d. L'axe $\Delta = (S, \overrightarrow{w})$ du cône est une bissectrice du couple de droites $(\mathcal{D}_1, \mathcal{D}_2)$, donc tout point de Δ est à égale distance des droites $\mathcal{D}_1$ et $\mathcal{D}_2$. Un point Ω sur Δ est le centre d'un cercle tangent aux droites $\mathcal{D}_1$, $\mathcal{D}_2$ et $\mathcal{D}$ si et seulement si il appartient à l'intersection de Δ et d'une bissectrice d_1 de $(\mathcal{D}, \mathcal{D}_1)$, ou bien à l'intersection de Δ et d'une bissectrice d_2 de $(\mathcal{D}, \mathcal{D}_2)$. On obtient ainsi deux points Ω_1 et Ω_2 (voir FIG. 5.3).
Les deux cercles obtenus sont les cercles exinscrits au triangle dont les côtés admettent les droites $\mathcal{D}_1$, $\mathcal{D}_2$ et $\mathcal{D}$ comme support, dont les centres appartiennent à la bissectrice extérieure Δ issue de S de ce triangle.
Il est facile de voir que les droites $\mathcal{D}$, $\mathcal{D}_1$, d_1 et $\mathcal{D}$, $\mathcal{D}_2$, d_2 sont symétriques par rapport à (SY), de sorte que les cercles tangents à ces droites soient aussi symétriques, et donc de même rayon ρ.

I.2.e. • Soit F_i le projeté de Ω_i sur $\mathcal{D}$ dans le plan $\mathcal{P}'$. Le plan $\mathcal{P}$ admettant l'équation cartésienne $Y = -\sqrt{10}/5$ dans le repère $\mathcal{R} = (S, \overrightarrow{u}, \overrightarrow{v}, \overrightarrow{w})$, la droite $(\Omega_i F_i)$ est perpendiculaire à $\mathcal{P}$. Comme $F_i \in \mathcal{P}$, on peut affirmer que F_i est le

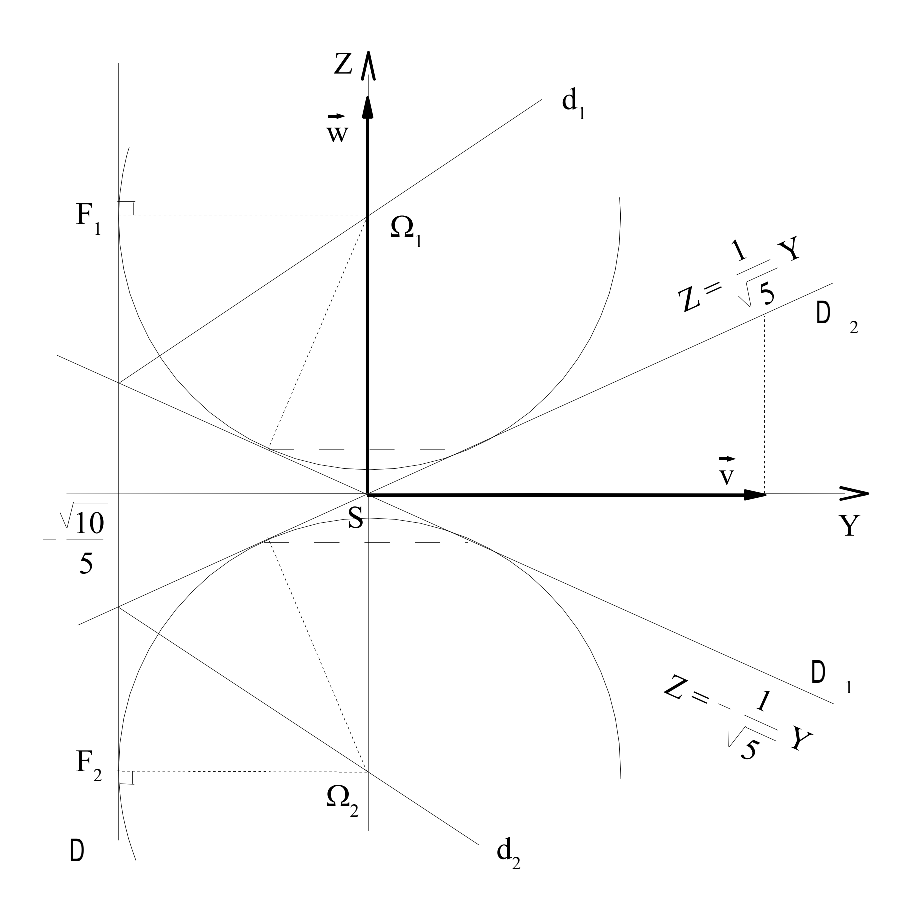


FIG. 5.3 – Figure complétée dans le plan $\mathcal{P}'$

projeté orthogonal de Ω_i sur $\mathcal{P}$. Cela prouve que la sphère $\mathcal{S}_i$ de centre Ω_i et de rayon ρ est tangente au plan $\mathcal{P}$.

• Par rotation autour de Δ, le cercle $\mathcal{C}(\Omega_i, \rho)$ de centre Ω_i et de rayon ρ, tangent à $\mathcal{D}_1$ et $\mathcal{D}_2$ engendre la sphère $\mathcal{S}_i$ qui sera tangente à la conique $\mathcal{Q}$, puisque $\mathcal{Q}$ est elle-même engendrée par la rotation des droites $\mathcal{D}_1$ et $\mathcal{D}_2$ autour de Δ (on dit que $\mathcal{D}_1$ et $\mathcal{D}_2$ sont des génératrices de $\mathcal{Q}$).

• La FIG. 5.3 montre les projetés F_1 et F_2 des centres Ω_1 et Ω_2 sur $\mathcal{P}$, ainsi que les projections des cercles $\mathcal{C}_1$ et $\mathcal{C}_2$ sur $\mathcal{P}'$, sous la forme de deux segments horizontaux tracés avec des tirets. La FIG. 5.4 permet d'avoir une idée de la situation réelle en dimension 3.

I.3.a. • Puisque $M \in \mathcal{C} = \mathcal{Q} \cap \mathcal{P}$, la droite (MS) joint un point du cône $\mathcal{Q}$ au sommet de ce cône, et à ce titre est entièrement incluse dans le cône. C'est

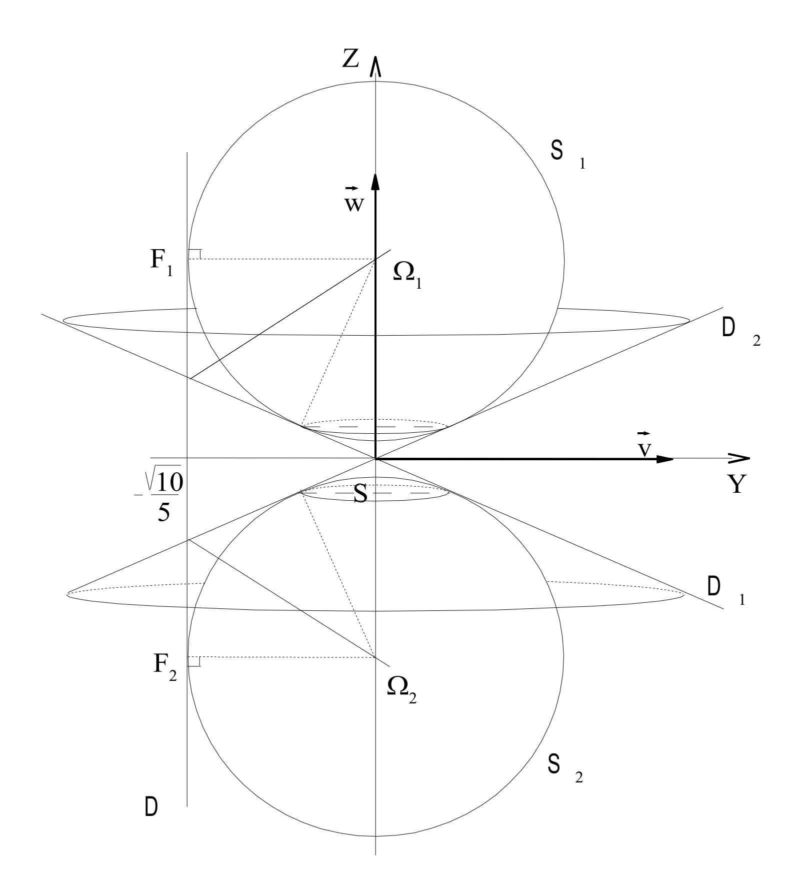


FIG. 5.4 – Situation générale

une directrice du cône, et en tant que telle, elle coupe les cercles de contact $\mathcal{C}_1$ et $\mathcal{C}_2$ en deux points T_1 et T_2.

• La droite (MF_1) est incluse dans le plan $\mathcal{P}$ tangent à $\mathcal{Q}$ en F_1, et passe par F_1. C'est donc une tangente à la sphère $\mathcal{S}_1$ issue de M. La droite (MT_1) coupe $\mathcal{S}_1$ en un unique point T_1. C'est donc aussi une tangente à $\mathcal{S}_1$ issue de M. Finalement (MF_1) et (MT_1) sont deux tangentes à la sphère $\mathcal{S}_1$ issue de M, donc $MT_1 = MF_1$. C'est une conséquence simple du Théorème de Pythagore (voir (FIG. 5.5) :

$$MT_1^2 = M\Omega_1^2 - \Omega T_1^2 = M\Omega_1^2 - \rho^2 = M\Omega_1^2 - F_1\Omega_1^2 = MF_1^2.$$

On montrerait de la même façon que $MT_2 = MF_2$.

• Montrons que $|MT_1 - MT_2|$ est constant.

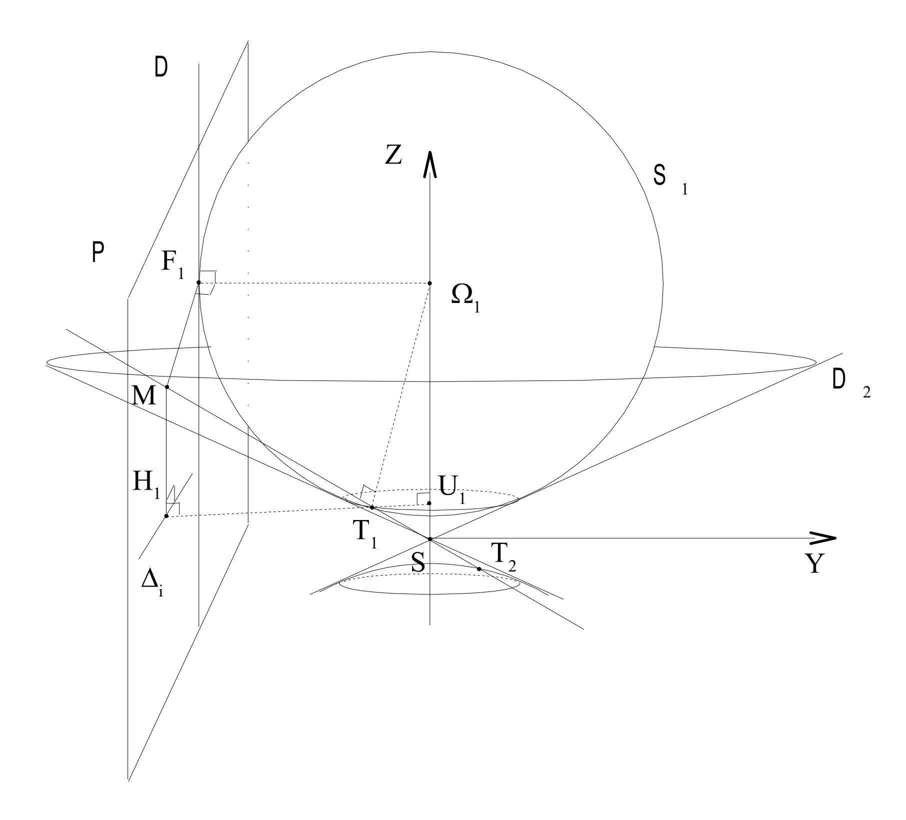


FIG. 5.5 – Les points M, S, H_1, T_1 et U_1 sont coplanaires

- Le point M appartient à $\mathcal{P}$, et les sphères $\mathcal{S}_1$ et $\mathcal{S}_2$ sont incluses dans le même demi-espace fermé E_S de frontière $\mathcal{P}$ (celui qui contient S), donc T_1 et T_2 appartiennent à E_S. Par convexité des demi-plans, $[T_1T_2] \subset E_S$, et cela prouve que $M \in (MS) \setminus]T_1T_2[$ (en effet, supposer que M appartient à $]T_1T_2[$ impose d'avoir T_1 et T_2 de part et d'autre de $\mathcal{P}$, ou sur la frontière $\mathcal{P}$ de ces demi-plans, ce qui n'est pas la cas).

- Ainsi $M \in (MS) \setminus]T_1T_2[$, et $|MT_1 - MT_2| = T_1T_2 = 2T_1S$, puisque T_1 et T_2 sont symétriques par rapport à S. Le Théorème de Pythagore appliqué au triangle rectangle Ω_1T_1S (FIG. 5.6) donne

$$T_1S^2 = \Omega_1S^2 - \Omega_1{T_1}^2 = \Omega_1S^2 - \rho^2,$$

et la quantité $|MT_1 - MT_2| = 2\sqrt{\Omega_1S^2 - \rho^2}$ reste constante lorsque M décrit l'hyperbole $\mathcal{C} = \mathcal{Q} \cap \mathcal{P}$.

- *Conclusion* : Posons $a = \sqrt{\Omega_1S^2 - \rho^2}$. On vient de prouver que l'implica-

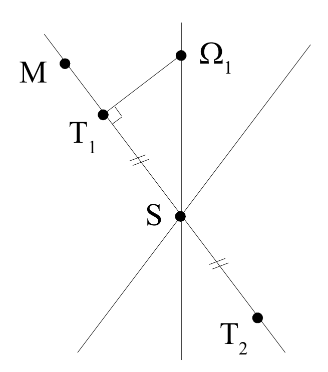


FIG. 5.6 – M n'est pas strictement entre T_1 et T_2

tion suivante est vraie pour tout point M du plan $\mathcal{P}$:

$$M \in \mathcal{C} \;\Rightarrow\; |MF_1 - MF_2| = 2a.$$

La condition $|MF_1 - MF_2| = 2a$ définit une hyperbole Λ de foyers F_1 et F_2 ([15], Section 20.2). On a donc $\mathcal{C} \subset \Lambda$. Comme deux hyperboles distinctes se coupent en au plus quatre points (voir remarque), on en déduit $\mathcal{C} = \Lambda$. On peut donc affirmer que :

▶ $M \in \mathcal{C} \;\Leftrightarrow\; |MF_1 - MF_2| = 2a$.

▶ $\mathcal{C}$ est l'hyperbole de foyers F_1 et F_2 (les points de contact des sphères $\mathcal{S}_1$ et $\mathcal{S}_2$ sur $\mathcal{P}$) et de demi-grand axe de longueur a.

Remarque : Il est bon de savoir démontrer que deux hyperboles distinctes se coupent en au plus quatre points. Cela peut servir à l'oral, et nécessite seulement de savoir qu'un polynôme à coefficients réels non nul de degré 4 admet au plus 4 racines. La preuve reprise ici est celle de la première question de l'exercice 80 de [16] que l'on pourra résoudre en entier pour s'entraîner sur les coniques. Les notations de la preuve suivante sont indépendantes de celles du problème.
Considérons une hyperbole H dessinée dans un plan $\mathcal{P}$. Cette hyperbole admet l'équation simple $xy = 1$ dans un repère $(O, \overrightarrow{i}, \overrightarrow{j})$ d'axes les asymptotes de H. Ce repère n'est ni normé, ni orthogonal, mais il suffit amplement pour dénombrer des points d'intersections. Considérons une autre conique (non dégénérée) H'. Celle-ci admet une équation du style

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

dans le repère $(O, \overrightarrow{i}, \overrightarrow{j})$, où $(a, b, c, d, e, f) \neq (0, 0, 0, 0, 0, 0)$. Si M désigne un

point de $\mathcal{P}$ de coordonnées (x,y) dans $(O,\overrightarrow{i},\overrightarrow{j})$,

$$M \in H \cap H' \Leftrightarrow \left\{ \begin{array}{l} xy = 1 \\ ax^2 + bxy + cy^2 + dx + ey + f = 0 \end{array} \right.$$
$$\Leftrightarrow \left\{ \begin{array}{l} xy = 1 \\ ax^2 + b + c\dfrac{1}{x^2} + dx + e\dfrac{1}{x} + f = 0 \end{array} \right.$$

et finalement

$$(E) \quad M \in H \cap H' \Leftrightarrow \left\{ \begin{array}{l} xy = 1 \\ ax^4 + dx^3 + (b+f)\,x^2 + ex + c = 0. \quad (*) \end{array} \right.$$

Si l'on note $P\,(x)$ la fonction polynomiale figurant dans le premier membre de $(*)$, on vient de prouver que :

> M appartient à $H \cap H'$ si et seulement si son abscisse x est une racine non nulle de P, et son ordonnée y est égale à l'inverse de son abscisse.

Si $H \cap H'$ est infini, le polynôme P de degré ≤ 4 admet une infinité de racines réelles, et c'est nécessairement le polynôme nul. Dans ce cas

$$a = d = b + f = e = c = 0$$

et H' admet l'équation $xy = 1$. On obtient bien $H' = H$, et l'on a montré l'implication

$$H \cap H' \text{ infini } \Rightarrow H' = H.$$

Si $H \neq H'$, la contraposée de l'implication précédente montre que $H \cap H'$ est un ensemble fini, et clairement P n'est pas identiquement nul et de degré inférieur ou égal à 4. Un polynôme non nul de degré au plus 4 admettant toujours moins de 4 racines dans $\mathbb{R}$, on peut affirmer que l'intersection $H \cap H'$ est de cardinal ≤ 4.

I.3.b. • Montrons que les points M, S, H_1, T_1, U_1 sont coplanaires.
Dans le repère $\mathcal{R} = (S,\overrightarrow{u},\overrightarrow{v},\overrightarrow{w})$, le plan $\mathcal{P}$ est vertical (puisque d'équation $Y = -\frac{\sqrt{10}}{5}$) et $\mathcal{C}_1$ est inclus dans un plan Π_1 horizontal. Donc $\Delta_1 = \mathcal{P} \cap \Pi_1$ est une droite horizontale. Comme H_1 est le projeté orthogonal de $M \in \mathcal{P}$ sur Δ_1, on en déduit que (MH_1) est verticale. Ainsi les droites (MH_1) et (SU_1), toutes deux verticales, sont parallèles, et les points M, S, H_1, U_1 appartiennent à un même plan Π. Comme $T_1 \in (MS) \subset \Pi$, ce sont les 5 points M, S, H_1, T_1, U_1 qui appartiennent à Π.

• Le Théorème de Thalès dans le triangle appliqué dans la FIG. 5.7 donne

$$\frac{MH_1}{MT_1} = \frac{SU_1}{ST_1} = \frac{d\,(S,\Pi_1)}{\sqrt{\Omega_1 S^2 - \rho^2}}.$$

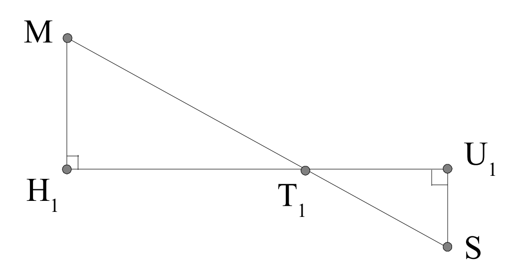


FIG. 5.7 – Situation de Thalès dans le plan Π

Le rapport MH_1/MT_1 reste donc égal à une constante $1/e$ ne dépendant que du plan $\mathcal{P}$ et du cône $\mathcal{Q}$ lorsque M parcourt l'hyperbole $\mathcal{C}$.

- *Conclusion* : Puisque $MT_1 = MF_1$, on obtient

$$M \in \mathcal{C} \;\Rightarrow\; \frac{MF_1}{MH_1} = e.$$

Mais l'ensemble des points M de $\mathcal{P}$ vérifiant l'égalité $MF_1/MH_1 = e$ est une conique Λ de foyer F_1 et de directrice Δ_1. Comme dans la question précédente, l'inclusion $\mathcal{C} \subset \Lambda$ est en fait une égalité, et l'on peut affirmer que :

- ▶ $M \in \mathcal{C} \;\Leftrightarrow\; MF_1/MH_1 = e$.
- ▶ $\mathcal{C}$ est l'hyperbole de $\mathcal{P}$ de foyer F_1, de directrice Δ_1 et d'excentricité e.

II.1.a. On a

$$\begin{aligned}\binom{n}{p-1} = \binom{n-1}{p} &\Leftrightarrow \frac{n!}{(p-1)!(n-p+1)!} = \frac{(n-1)!}{p!(n-p-1)!}\\ &\Leftrightarrow np = (n-p+1)(n-p)\\ &\Leftrightarrow n^2 + p^2 - 3np + n - p = 0\end{aligned}$$

avec les conditions usuelles d'existence des symboles $\binom{n}{p-1}$ et $\binom{n-1}{p}$, soit

$$\left\{\begin{array}{l} 0 \leq p-1 \leq n \\ 0 \leq p \leq n-1 \end{array}\right., \text{ ce qui équivaut à } 2 \leq p+1 \leq n.$$

L'équation (Σ_1) est bien équivalente au système

$$(\Sigma_2) \quad \left\{\begin{array}{l} 2 \leq p+1 \leq n \\ n^2 + p^2 - 3np + n - p = 0. \end{array}\right.$$

II.1.b. • Le discriminant de l'équation $X^2 - (3n+1)X + n^2 + n = 0$ est $\Delta = (3n+1)^2 - 4\left(n^2+n\right) = 5n^2 + 2n + 1$. Le discriminant de $5n^2 + 2n + 1$ est $\delta = -4 < 0$, donc Δ reste strictement positif pour tout réel n. L'équation proposée admet donc toujours deux solutions réelles distinctes

$$X_1 = \frac{a_n - \sqrt{b_n}}{2} \quad \text{et} \quad X_2 = \frac{a_n + \sqrt{b_n}}{2}$$

où $a_n = 3n + 1$ et $b_n = 5n^2 + 2n + 1$.

• On a

$$\begin{aligned} 2 \leq X_1 + 1 \leq n &\Leftrightarrow 2 \leq a_n - \sqrt{b_n} \leq 2n - 2 \\ &\Leftrightarrow n + 3 \leq \sqrt{b_n} \leq 3n - 1 \\ &\Leftrightarrow (n+3)^2 \leq 5n^2 + 2n + 1 \leq (3n-1)^2 . \end{aligned}$$

Après simplifications,

$$2 \leq X_1 + 1 \leq n \;\Leftrightarrow\; \begin{cases} 2 \leq n \\ 0 \leq 4\,(n+1)\,(n-2) \end{cases} \;\Leftrightarrow\; 2 \leq n$$

puisque le trinôme $(n+1)\,(n-2)$ reste positif lorsque n est à l'extérieur des racines -1 et 2.

• En recommençant avec X_2, on obtient

$$2 \leq X_2 + 1 \leq n \;\Leftrightarrow\; 1 - 3n \leq \sqrt{b_n} \leq -n - 3.$$

Comme le radical $\sqrt{b_n}$ est toujours positif, l'inégalité $\sqrt{b_n} \leq -n - 3$ sera impossible à satisfaire quel que soit la valeur de l'entier n.

• *En conclusion* : $2 \leq X_1 + 1 \leq n$ si et seulement si $n \geq 2$, et l'on n'a jamais $2 \leq X_2 + 1 \leq n$.

II.1.c. Si b est un carré parfait, il existe un entier naturel m tel que $b = m^2$, et $\sqrt{b} = m$ est un entier, donc un nombre rationnel. Réciproquement, si $\sqrt{b}$ est un rationnel, il existe deux entiers naturels p et q premiers entre eux, avec $q \neq 0$, tels que $\sqrt{b} = p/q$. Dans ce cas, $q^2 b = p^2$, et q divise p^2. Comme q est premier avec p, il sera aussi premier avec p^2, et le Théorème de Gauss montre que q divise 1 (en effet : q divise $p^2 \times 1$ et q premier avec p^2, donc q divise 1). Mais alors $q = 1$ et $b = p^2$ est un carré parfait.

II.1.d. L'équation (Σ_1) équivaut au système (Σ_2) d'après II.1.a. Donc

$$(n,p) \text{ solution de } (\Sigma_1) \quad \Rightarrow \quad (2 \leq n \text{ et } p \in \{X_1, X_2\}) .$$

Mais p ne peut être égal à X_2, puisque $2 \leq X_2 + 1 \leq n$ n'est jamais satisfait d'après II.1.b. Donc

$$p = X_1 = \frac{a_n - \sqrt{b_n}}{2}$$

et $\sqrt{b_n} = a_n - 2p$ est un entier. II.1.c impose alors à $b_n = 5n^2 + 2n + 1$ d'être un carré parfait. On retiendra

$$p = \frac{3n + 1 - \sqrt{5n^2 + 2n + 1}}{2}.$$

II.1.e. Les questions I.1.a et I.1.b permettent d'écrire

$$\begin{aligned}
(n,p) \text{ solution de } (\Sigma_1) &\Leftrightarrow \begin{cases} 2 \leq p + 1 \leq n \\ n^2 + p^2 - 3np + n - p = 0 \end{cases} \\
&\Leftrightarrow \begin{cases} 2 \leq p + 1 \leq n \\ p \in \{X_1, X_2\} \end{cases} \\
&\Leftrightarrow \begin{cases} 2 \leq X_1 + 1 \leq n \\ p = X_1 \end{cases} \quad \Leftrightarrow \begin{cases} 2 \leq n \\ p = X_1. \end{cases}
\end{aligned}$$

Si l'on suppose $n \geq 2$ et que $b_n = 5n^2 + 2n + 1$ est un carré parfait, on obtient

$$(n,p) \text{ solution de } (\Sigma_1) \ \Leftrightarrow \ p = X_1 = \frac{a_n - \sqrt{b_n}}{2}.$$

S'il existe p tel que (n,p) soit solution de (Σ_1), ce p est unique et donné par l'égalité ci-dessus. Pour conclure, il faut encore vérifier que p est bien entier, autrement dit que $a_n - \sqrt{b_n}$ est toujours pair. Puisqu'un entier est toujours de même parité que son carré, on a les congruences suivantes modulo 2 :

$$a_n - \sqrt{b_n} \equiv a_n - b_n \equiv 3n + 1 - \left(5n^2 + 2n + 1\right) \equiv n + 1 - (n+1) \equiv 0 \ \ (2)$$

et l'on peut conclure.

II.1.f. Pour chaque entier n appartenant à $[2, n_0]$, on calcule $b_n = 5n^2 + 2n + 1$ et l'on cherche si b_n est un carré parfait. Si oui, on obtient un couple-solution

$$(n,p) = \left(n, \frac{3n + 1 - \sqrt{5n^2 + 2n + 1}}{2}\right)$$

de (Σ_1). Voici un algorithme possible :

Lire n_0,
Pour n variant de 2 à n_0,
  Calculer $b_n = 5n^2 + 2n + 1$,

Si b_n n'est pas un carré parfait, passer au n suivant,
Sinon calculer $p = (3n + 1 - \sqrt{b_n})/2$, imprimer (n, p), puis passer au n suivant.

Remarque : Sur MuPad Light, le programme peut s'écrire ainsi :

```
for n from 2 to 10000 do
b :=5*n^2+2*n+1 : c :=sqrt(b) :
if float(c-floor(c))<10^(-5) then print(n,(3*n+1-c)/2)
end_if :
end_for
```

et l'on obtient la sortie suivante :

```
2, 1
15, 6
104, 40
714, 273
4895, 1870
```

II.2.a. Dans la question II.1.a, on a déjà vérifié que $\binom{n}{p-1} = \binom{n-1}{p}$ s'écrivait $np = (n - p + 1)(n - p)$, ou encore $n^2 + p^2 - 3np + n - p = 0$. Par suite

$$n^2 - 3np + n = p\,(1 - p)$$

et n divise $p\,(1 - p)$. Comme n est premier avec p, le Théorème de Gauss montre que n divise $p - 1$, et il existe un entier k tel que $p - 1 = kn$. Pour être solution de (Σ_1), le couple (n, p) doit aussi vérifier les inégalités $2 \leq p + 1 \leq n$, ce qui s'écrit $2 \leq kn + 2 \leq n$, ou encore $0 \leq kn \leq n - 2$. Cela entraîne $k = 0$ (en effet, $0 \leq kn$ montre que k doit être positif, et supposer $1 \leq k$ entraîne $n \leq kn \leq n - 2$, soit $0 \leq -2$, ce qui est absurde) donc $p = 1$ et $n = 2$.
En conclusion, il existe une unique solution (n, p) de (Σ_1) formée d'entiers premiers entre eux, c'est $(2, 1)$.

Remarque : Voici une autre façon de vérifier que n divise $p\,(1 - p)$. Comme $np = (n - p + 1)(n - p)$, l'entier n divise le produit $(n - p + 1)(n - p)$. Mais n est premier avec p, donc premier avec $n - p$ (en effet, les diviseurs communs à n et p d'une part, et à n et $n - p$ d'autre part, coïncident), et le Théorème de Gauss montre que n divise $n - p + 1$, donc aussi $p - 1$.

II.2.b. Ici $r = n \wedge p$, $n = ru$ et $p = rv$. La question II.1.a nous offre deux traductions du problème (Σ_1) :

$$(\Sigma_1) \;\Leftrightarrow\; \begin{cases} 2 \leq p + 1 \leq n \\ n^2 + p^2 - 3np + n - p = 0 \end{cases} \;\Leftrightarrow\; \begin{cases} 2 \leq p + 1 \leq n \\ np = (n - p)\,(n - p + 1)\,. \end{cases}$$

• En remplaçant,

$$r^2uv = r\,(u-v)\,(r\,(u-v)+1)$$
$$ruv - (u-v)^2\,r = u-v$$
$$r\left(3uv - u^2 - v^2\right) = u - v \quad (*)$$

donc $\boxed{r \text{ divise } u-v}$.

• Supposons par l'absurde que r divise $u-v$ tout en étant différent de $u-v$. Dans ce cas, il existe $k \in \mathbb{N}^*$ tel que $u-v = kr$, et comme tout entier naturel différent de 1, k possède un diviseur premier t. Si l'on note t^α $(\alpha \in \mathbb{N})$ la partie de la décomposition en facteurs premiers de r contenant ce diviseur premier t, on a

$$\begin{cases} t^{\alpha+1} \,|\, u-v \\ t^{\alpha+1} \nmid r \\ t^\alpha \,|\, r, \end{cases}$$

où | représente la relation "divise".
Comme $t^\alpha \,|\, r$ et $r = n \wedge p$, on déduit que t^α divise n et p. Il existe donc deux entiers n' et p' tels que $n = t^\alpha n'$ et $p = t^\alpha p'$.
De $np = r\,(u-v)\,(r\,(u-v)+1)$, on déduit

$$t^{2\alpha+1} \,|\, r\,(u-v) \,|\, np = t^{2\alpha} n'p'$$

de sorte que t divise le produit $n'p'$. Mais t, premier, divisera alors l'un des termes n' ou p' du produit. Supposons par exemple que t divise n' (le raisonnement serait identique dans l'autre cas). Comme $n - p = r\,(u-v)$,

$$t^{\alpha+1} \,|\, (u-v) \,|\, n-p \;\Rightarrow\; t^{\alpha+1} \,|\, t^\alpha(n'-p') \;\Rightarrow\; t \,|\, (n'-p').$$

De $t \,|\, n'$ et $t \,|\, (n'-p')$ on déduit $t \,|\, n'$ et $t \,|\, p'$, puis $t^{\alpha+1} \,|\, n$ et $t^{\alpha+1} \,|\, p$. Cela prouve que $t^{\alpha+1}$ divise le pgcd $r = n \wedge p$, en contradiction avec notre choix de t et de α. En conclusion $\boxed{r = u-v}$.

• Puisque $r = u - v$, $(*)$ devient successivement

$$3uv - u^2 - v^2 = 1$$
$$3\,(r+v)\,v - (r+v)^2 - v^2 = 1$$
$$v^2 + rv - r^2 - 1 = 0.$$

Le discriminant de l'équation du second degré que l'on vient d'obtenir est $\Delta = r^2 + 4\left(r^2+1\right) = 5r^2 + 4$. Il est toujours strictement positif, donc l'équation

admet deux solutions réelles $v = (-r \pm \sqrt{5r^2+4})/2$. Comme v doit être positif, on ne retient que la solution

$$v = \frac{\sqrt{5r^2+4}-r}{2}.$$

- Comme $5r^2+4 > 5r^2$,

$$p = rv = r\frac{\sqrt{5r^2+4}-r}{2} > r\frac{r\sqrt{5}-r}{2} \Rightarrow r^2 < \frac{2p}{\sqrt{5}-1}.$$

II.2.c. Lorsque $2 \leq n \leq 105$, la condition

$$r^2 < \frac{2p}{\sqrt{5}-1} \leq \frac{2n}{\sqrt{5}-1} \leq \frac{2 \times 105}{\sqrt{5}-1}$$

entraîne

$$r < \sqrt{\frac{2 \times 105}{\sqrt{5}-1}} \simeq 13,034$$

et restreint nos recherches. Pour chaque entier r appartenant à l'intervalle $[1, 13]$, nous calculons

$$v = \frac{\sqrt{5r^2+4}-r}{2}. \quad (\dagger)$$

Si v n'est pas entier, nous passons à l'entier r suivant. Si v est entier, nous calculons $u = v + r$. Si u et v sont premiers entre eux, nous obtenons un couple-solution $(n,p) = (ru, rv)$.
La question II.2.b montre effectivement qu'une solution de (Σ_1) est de cette forme. Mais la réciproque est vraie (lorsqu'on a vérifié tous les points précédents) puisque $(\dagger)$ équivaut à l'équation $n^2+p^2-3np+n-p=0$ du système équivalent au problème (Σ_1) écrit en II.1.a, et que les inégalités $2 \leq p+1 \leq n$ sont alors toujours vraies, comme on le vérifie facilement :

$$2 \leq p+1 \Leftrightarrow 2 \leq r\frac{\sqrt{5r^2+4}-r}{2}+1 \Leftrightarrow 1 \leq r^2 \text{ (vraie)}$$

et

$$p+1 \leq n \Leftrightarrow rv+1 \leq r(v+r) \Leftrightarrow 1 \leq r^2 \text{ (vraie).}$$

Calculons $f(r) = 5r^2+4$ pour chaque entier r de l'intervalle $[1, 13]$:

r	1	2	3	4	5	6	7	8	9	10	11	12	13
$f(r)$	9	24	49	84	129	184	249	324	409	504	609	724	849

$f(r)$ est un carré parfait seulement lorsque $r = 1$, 3 ou 8.

- Si $r = 1$, $v = 1$, $u = 2$, donc $(n, p) = (2, 1)$,
- Si $r = 3$, $v = 2$, $u = 5$, donc $(n, p) = (15, 6)$,
- Si $r = 8$, $v = 5$, $u = 13$, donc $(n, p) = (104, 40)$.

Les trois couples (n, p) ci-dessus sont les seuls couples-solutions de (Σ_1) lorsque $2 \leq n \leq 105$.

III.1.a. Une équation de $\mathcal{C}$ dans le repère $\mathcal{R}_0 = (O, \overrightarrow{i}, \overrightarrow{j})$ est

$$\mathcal{C} : \quad x^2 - 3xy + y^2 + x - y = 0.$$

Les formules de changement de repère de $\mathcal{R}_0$ vers $(I, \overrightarrow{i}, \overrightarrow{j})$ sont

$$\begin{cases} x = x_1 - \dfrac{1}{5} \\ y = y_1 + \dfrac{1}{5}, \end{cases}$$

donc $\mathcal{C}$ admettra l'équation

$$\left(x_1 - \frac{1}{5}\right)^2 - 3\left(x_1 - \frac{1}{5}\right)\left(y_1 + \frac{1}{5}\right) + \left(y_1 + \frac{1}{5}\right)^2 + x_1 - y_1 - \frac{2}{5} = 0$$

dans le nouveau repère $(I, \overrightarrow{i}, \overrightarrow{j})$, ou encore

$$\mathcal{C} : \quad x_1^2 - 3x_1y_1 + y_1^2 - \frac{1}{5} = 0.$$

III.1.b.

$$\begin{aligned} a^2 + b^2 - 3ab &= \left(b - \frac{3}{2}a\right)^2 - \frac{9}{4}a^2 + a^2 \\ &= \left(b - \frac{3}{2}a\right)^2 - \frac{5}{4}a^2 = \left(b - \frac{3-\sqrt{5}}{2}a\right)\left(b - \frac{3+\sqrt{5}}{2}a\right). \end{aligned}$$

III.1.c. L'équation de $\mathcal{C}$ s'écrit

$$\mathcal{C} : \quad \left(y_1 - \frac{3-\sqrt{5}}{2}x_1\right)\left(y_1 - \frac{3+\sqrt{5}}{2}x_1\right) - \frac{1}{5} = 0,$$

ou encore $\mathcal{C} : \ 5XY + 1 = 0$ en posant

$$\begin{cases} X = \dfrac{\sqrt{5}+3}{2}x_1 - y_1 \\ Y = \dfrac{\sqrt{5}-3}{2}x_1 + y_1. \end{cases}$$

Ces dernières formules correspondent bien à un nouveau changement de repère, du repère $(I, \overrightarrow{i}, \overrightarrow{j})$ vers un repère $\mathcal{R}_1 = (I, \overrightarrow{u}, \overrightarrow{v})$, car constituent un système de Cramer en (x_1, y_1) (il est facile de vérifier que le déterminant de ce système n'est pas nul). En posant $\alpha = \frac{\sqrt{5}+3}{2}$ et $\beta = \frac{\sqrt{5}-3}{2}$, on obtient $\alpha + \beta = \sqrt{5} > 0$ et

$$\left\{ \begin{array}{l} X = \alpha \left(x + \dfrac{1}{5} \right) - \left(y - \dfrac{1}{5} \right) \\ Y = \beta \left(x + \dfrac{1}{5} \right) + \left(y - \dfrac{1}{5} \right). \end{array} \right.$$

Résolvons ce système en x, y :

$$\left\{ \begin{array}{l} \alpha x - y = X - \dfrac{\alpha}{5} - \dfrac{1}{5} \\ \beta x + y = Y - \dfrac{\beta}{5} + \dfrac{1}{5}. \end{array} \right.$$

entraîne

$$x = \frac{1}{\sqrt{5}} \left(X + Y - \frac{\sqrt{5}}{5} \right) = \frac{\sqrt{5}}{5} X + \frac{\sqrt{5}}{5} Y - \frac{1}{5}$$

et

$$\begin{aligned} y = \alpha x - X + \frac{\alpha}{5} + \frac{1}{5} &= \alpha \left(\frac{\sqrt{5}}{5} X + \frac{\sqrt{5}}{5} Y - \frac{1}{5} \right) - X + \frac{\alpha}{5} + \frac{1}{5} \\ &= \left(\frac{\alpha\sqrt{5}}{5} - 1 \right) X + \frac{\alpha\sqrt{5}}{5} Y + \frac{1}{5} \\ &= \frac{3\sqrt{5}-5}{10} X + \frac{3\sqrt{5}+5}{10} Y + \frac{1}{5}. \end{aligned}$$

Les formules de changement de repère de $\mathcal{R}_0 = (O, \overrightarrow{i}, \overrightarrow{j})$ vers $\mathcal{R}_1 = (I, \overrightarrow{u}, \overrightarrow{v})$ sont donc

$$\left\{ \begin{array}{l} x = \dfrac{\sqrt{5}}{5} X + \dfrac{\sqrt{5}}{5} Y - \dfrac{1}{5} \\ y = \dfrac{3\sqrt{5}-5}{10} X + \dfrac{3\sqrt{5}+5}{10} Y + \dfrac{1}{5}. \end{array} \right.$$

Une hyperbole admet une équation de la forme $XY = cte$ dans un repère donné si et seulement si elle admet les axes du repère pour asymptotes. Les axes $(I, \overrightarrow{u})$ et $(I, \overrightarrow{v})$ du repère $\mathcal{R}_1$ représentent donc les asymptotes de $\mathcal{C}$.

Remarque : La matrice de passage de la base $(\overrightarrow{i}, \overrightarrow{j})$ vers la base $(\overrightarrow{u}, \overrightarrow{v})$ est

$$\begin{pmatrix} \dfrac{\sqrt{5}}{5} & \dfrac{\sqrt{5}}{5} \\ \dfrac{3\sqrt{5}-5}{10} & \dfrac{3\sqrt{5}+5}{10} \end{pmatrix},$$

et les colonnes de cette matrice sont formées des coordonnées de $\overrightarrow{u}$ et $\overrightarrow{v}$ dans l'ancienne base $(\overrightarrow{i}, \overrightarrow{j})$.

III.2.a. L'image de l'hyperbole $\mathcal{C}$ par une application affine bijective h est une hyperbole $h(\mathcal{C})$, et l'on sait que deux hyperboles se coupent en au plus quatre points. L'inclusion $h(\mathcal{C}) \subset \mathcal{C}$ entraîne donc l'égalité $h(\mathcal{C}) = \mathcal{C}$, c'est-à-dire $h \in G_1$.
Le réciproque est triviale : si $h \in G_1$, $h(\mathcal{C}) = \mathcal{C}$ donc a fortiori $h(\mathcal{C}) \subset \mathcal{C}$.

Remarque : Le lecteur pourra se poser la question de savoir comment démontrer que l'image d'une conique par une bijection affine est une conique du même type (solution à la Section 5.3.1).

III.2.b. L'ensemble G_1 est inclus dans $\mathrm{GA}(\mathcal{P})$ et n'est pas vide, car contient l'identité. Si $h \in G_1$, alors h est une bijection affine d'inverse h^{-1} et $h(\mathcal{C}) = \mathcal{C}$ entraîne $h^{-1}(\mathcal{C}) = \mathcal{C}$, donc $h^{-1} \in G_1$. Enfin, si $h, l \in G_1$, la composée $h \circ l$ est encore une bijection affine et vérifie $(h \circ l)(\mathcal{C}) = h(l(\mathcal{C})) = h(\mathcal{C}) = \mathcal{C}$, donc appartient à G_1. L'ensemble G_1 est donc bien un sous-groupe de $\mathrm{GA}(\mathcal{P})$.

III.2.c. Par définition, une application h de $\mathcal{P}$ dans $\mathcal{P}$ est affine si et seulement si il existe un endomorphisme l de P tel que

$$\forall M \in \mathcal{P} \qquad \overrightarrow{f(I)\,f(M)} = l(\overrightarrow{IM}). \quad (\dagger)$$

On dit alors que l est la partie linéaire de h (ou l'application linéaire associée à h). Si

$$M = \begin{pmatrix} a & b \\ d & e \end{pmatrix}$$

désigne la matrice de l dans la base $(\overrightarrow{u}, \overrightarrow{v})$, et si (c, f) représentent les coordonnées de $f(I)$ dans le repère $\mathcal{R}_1 = (I, \overrightarrow{u}, \overrightarrow{v})$, la traduction matricielle de $(\dagger)$ est

$$\begin{pmatrix} X' \\ Y' \end{pmatrix} = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} c \\ f \end{pmatrix},$$

ce qui s'écrit encore

$$\begin{cases} X' = aX + bY + c \\ Y' = dX + eY + f. \end{cases}$$

D'après le cours, h est bijective si et seulement si sa partie linéaire l est bijective, ce qui équivaut à $\det M \neq 0$, soit $ae - bd \neq 0$.

III.2.d. L'équation de $\mathcal{C}$ dans $\mathcal{R}_1$ est $5XY + 1 = 0$. L'application h appartient à G_1 si et seulement si $h(\mathcal{C}) \subset \mathcal{C}$, c'est-à-dire si et seulement si

$$\forall (X, Y) \in \mathbb{R}^2 \qquad 5XY + 1 = 0 \ \Rightarrow\ 5X'Y' + 1 = 0.$$

Pour tout $X \in \mathbb{R}^*$, on doit donc avoir

$$5\left(aX - \frac{b}{5X} + c\right)\left(dX - \frac{e}{5X} + f\right) + 1 = 0$$

$$\left(5aX^2 + 5cX - b\right)\left(5dX^2 + 5fX - e\right) + 5X^2 = 0$$

$$25adX^4 + (25cd + 25af)\,X^3 + (25cf - 5bd - 5ae + 5)\,X^2 \\ - (5bf + 5ce)\,X + be = 0.$$

Le polynôme apparaissant au premier membre est de degré ≤ 4 et admet pourtant une infinité de racines : il s'agit donc du polynôme nul. En rappelant que $ae - bd \neq 0$, on obtient

$$(S) \quad \begin{cases} ad = af + cd = bf + ce = be = 0 \\ 5cf - ae - bd = -1 \\ ae - bd \neq 0. \end{cases}$$

La réciproque est triviale : si (a, b, c, d, e, f) est solution de (S), alors $h \in G_1$. On retiendra :

$$h \in G_1 \iff (a, b, c, d, e, f) \text{ solution de } (S)\,.$$

III.2.e. • On résout le système (S). Puisque $ad = be = 0$, on envisage 4 cas.

α) Si $a = b = 0$, $ae - bd = 0$ et le système (S) n'a pas de solution.

β) Si $d = e = 0$, $ae - bd = 0$ donc (S) n'admet pas de solution.

γ) Si $a = e = 0$,

$$(S) \iff \begin{cases} cd = bf = 0 \\ 5cf - bd = -1 \\ bd \neq 0. \end{cases} \iff \begin{cases} c = f = 0 \\ d = 1/b \\ b \neq 0. \end{cases}$$

Les transformations h associées à ces coefficients sont de la forme

$$h_{1,\mu} \quad \begin{array}{ccc} \mathcal{P} & \to & \mathcal{P} \\ M\,(X, Y)_{\mathcal{R}_1} & \mapsto & M'\,(\mu Y, X/\mu)_{\mathcal{R}_1} \end{array}$$

avec $\mu \in \mathbb{R}^*$.

δ) Si $d = b = 0$, (S) devient

$$(S) \iff \begin{cases} af = ce = 0 \\ 5cf - ae = -1 \\ ae \neq 0. \end{cases} \iff \begin{cases} f = c = 0 \\ e = 1/a \\ ae \neq 0. \end{cases}$$

Les transformations h associées sont maintenant de la forme

$$\begin{array}{cccc} h_{2,\mu} & \mathcal{P} & \to & \mathcal{P} \\ & M\,(X,Y)_{\mathcal{R}_1} & \mapsto & M'\,(\mu X, Y/\mu)_{\mathcal{R}_1} \end{array}$$

avec $\mu \in \mathbb{R}^*$.

• Un théorème classique du cours ([15], Corollaire 7) montre qu'une application affine est une symétrie si et seulement si elle est involutive. Les applications $h_{1,\mu}$ sont clairement involutives, donc il s'agit toujours de symétries. Par contre

$$\begin{aligned} h_{2,\mu}^2 = Id &\Leftrightarrow \ \forall\,(X,Y) \in \mathbb{R}^2 \quad (X,Y) = \left(\mu^2 X, Y/\mu^2\right) \\ &\Leftrightarrow \ \mu^2 = 1 \ \Leftrightarrow \ \mu = \pm 1. \end{aligned}$$

$h_{2,\mu}$ est donc une symétrie si et seulement si il s'agit de l'identité ou de la symétrie par rapport au point I (on remarque en effet que toutes les transformations obtenues admettent I comme point invariant, puisque $f = c = 0$).

III.2.f. L'application

$$\begin{array}{cccc} \Phi : & (\mathrm{GA}\,(\mathcal{P})\,, \circ) & \longrightarrow & (\mathrm{GL}_2(\mathbb{R}), \times) \\ & h & \longmapsto & \Phi\,(h) \end{array}$$

qui à une bijection affine h fait correspondre la matrice de la partie linéaire de h dans la base $(\overrightarrow{u}, \overrightarrow{v})$, est un homomorphisme de groupes. On vient juste de démontrer que le sous-groupe G_1 de $\mathrm{GA}\,(\mathcal{P})$ est formé des bijections affines $h_{1,\mu}$ et $h_{2,\mu}$ dont les matrices dans la base $(\overrightarrow{u}, \overrightarrow{v})$ sont de la forme

$$\begin{pmatrix} \mu & 0 \\ 0 & 1/\mu \end{pmatrix} \quad \text{ou} \quad \begin{pmatrix} 0 & \mu \\ 1/\mu & 0 \end{pmatrix},$$

lorsque μ décrit $\mathbb{R}$. Par conséquent $G_1' = \Phi\,(G_1)$ et G_1' est un groupe comme l'image d'une sous-groupe de $\mathrm{GA}\,(\mathcal{P})$ par un homomorphisme de groupes. On constate aussi que la restriction

$$\begin{array}{cccc} \Phi|_{G_1} : & G_1 & \longrightarrow & G_1' \\ & h & \longmapsto & \Phi\,(h) \end{array}$$

de Φ à G_1 est un isomorphisme de groupes (restreinte au départ et à l'arrivée). C'est évidemment un morphisme surjectif, et l'injectivité est facile à prouver : si h et h' appartiennent à G_1 et ont même image par Φ, ce sont deux applications affines ayant même partie linéaire, et coïncidant en I (puisque I est invariant par tout élément de G_1), donc deux applications égales. L'isomorphisme proposé par l'énoncé est exactement $(\Phi|_{G_1})^{-1}$.

III.3.a. Il semble que non ! L'homothétie h de centre O et de rapport 2 transforme très certainement tout point $M(x,y)_{\mathcal{R}_0}$ à coordonnées entières en un point à coordonnées entières, donc $h(\mathcal{Z}) \subset \mathcal{Z}$. Malheureusement $N(1,1)_{\mathcal{R}_0}$ appartient à $\mathcal{Z}$, mais admet un unique antécédent de coordonnées $(1/2, 1/2)_{\mathcal{R}_0}$ non entières, donc $h(\mathcal{Z}) \neq \mathcal{Z}$.

III.3.b. G_2 est une partie non vide de $\mathrm{GA}(\mathcal{P})$ puique elle contient l'identité. Si h et l sont deux bijections affines de $\mathcal{P}$,

$$h \in G_2 \;\Leftrightarrow\; h(\mathcal{Z}) = \mathcal{Z} \;\Leftrightarrow\; \mathcal{Z} = h^{-1}(\mathcal{Z}) \;\Leftrightarrow\; h^{-1} \in G_2$$

et

$$h, l \in G_2 \;\Rightarrow\; (h \circ l)(\mathcal{Z}) = h(l(\mathcal{Z})) = h(\mathcal{Z}) = \mathcal{Z} \;\Rightarrow\; h \circ l \in G_2,$$

et cela prouve que G_2 est un sous-groupe de $\mathrm{GA}(\mathcal{P})$.

III.3.c. Une application h de $\mathrm{GA}(\mathcal{P})$ admet toujours une expression analytique est de la forme

$$(\spadesuit) \qquad \begin{cases} x' = ax + by + c \\ y' = dx + ey + f \end{cases}$$

dans le repère $\mathcal{R}_0$, avec $ae - bd \neq 0$, et l'on a

$$h \in G_2 \;\Leftrightarrow\; h(\mathcal{Z}) = \mathcal{Z} \;\Leftrightarrow\; \begin{cases} h(\mathcal{Z}) \subset \mathcal{Z} \\ \mathcal{Z} \subset h(\mathcal{Z}) \end{cases} \;\Leftrightarrow\; \begin{cases} h(\mathcal{Z}) \subset \mathcal{Z} \\ h^{-1}(\mathcal{Z}) \subset \mathcal{Z}. \end{cases}$$

Le système $(\spadesuit)$ s'inverse facilement en utilisant les formules de Cramer, et nous donne accès à l'expression analytique de h^{-1}. On trouve

$$x = \frac{1}{\Delta}\begin{vmatrix} x' - c & b \\ y' - f & e \end{vmatrix} \quad \text{et} \quad y = \frac{1}{\Delta}\begin{vmatrix} a & x' - c \\ d & y' - f \end{vmatrix}$$

où $\Delta = ae - bd$ est le déterminant du système. On peut donc affirmer que $h \in G_2$ si et seulement si les conditions $(C1)$ et $(C2)$ suivantes sont vérifiées :

$$(C1) \quad (x,y) \in \mathbb{Z}^2 \Rightarrow (ax + by + c, dx + ey + f) \in \mathbb{Z}^2\,;$$

$$(C2) \quad (x',y') \in \mathbb{Z}^2 \Rightarrow \left(\frac{1}{\Delta}\begin{vmatrix} x' - c & b \\ y' - f & e \end{vmatrix}, \frac{1}{\Delta}\begin{vmatrix} a & x' - c \\ d & y' - f \end{vmatrix}\right) \in \mathbb{Z}^2.$$

• Si $h \in G_2$, il suffit d'appliquer $(C1)$ avec (x,y) égal successivement à $(0,0)$, $(1,0)$ puis $(0,1)$ pour que c, f, $a+c$, $d+f$, $b+c$, $e+f$ soient tous entiers, d'où l'on déduit $(a,b,c,d,e,f) \in \mathbb{Z}^6$.

Comme $\Delta = ae - bd$ n'est pas nul, b et e ne peuvent pas être nuls en même temps.

- Si $b \neq 0$, on applique $(C2)$ avec $(x', y') = (c, f + \frac{1}{b})$. On obtient

$$\frac{1}{\Delta}\begin{vmatrix} 0 & b \\ 1/b & e \end{vmatrix} = \frac{-1}{\Delta} \in \mathbb{Z}$$

donc $\Delta = \pm 1$.

- Si $e \neq 0$, on applique $(C2)$ avec $(x', y') = (c + \frac{1}{e}, f)$ pour obtenir

$$\frac{1}{\Delta}\begin{vmatrix} 1/e & b \\ 0 & e \end{vmatrix} = \frac{1}{\Delta} \in \mathbb{Z}$$

donc $\Delta = \pm 1$.

Finalement, si $h \in G_2$, alors $(a, b, c, d, e, f) \in \mathbb{Z}^6$ et $\Delta = \pm 1$.

• Réciproquement, si $(a, b, c, d, e, f) \in \mathbb{Z}^6$ et $\Delta = \pm 1$, l'implication $(C1)$ est trivialement vérifiée. Et l'implication $(C2)$ est vraie puisque $\Delta = \pm 1$ et que tous les coefficients des déterminants sont entiers. On peut donc affirmer que h appartient à G_2.

Remarque : Pour montrer le sens direct, on peut utiliser les matrices

$$M = \begin{pmatrix} a & b \\ d & e \end{pmatrix} \quad \text{et} \quad M' = \begin{pmatrix} a' & b' \\ d' & e' \end{pmatrix}$$

des parties linéaires de h et h^{-1}. Supposons que h appartiennent à G_2. Après avoir vérifié, comme nous l'avons fait, que $(a, b, c, d, e, f) \in \mathbb{Z}^6$, on applique ce résultat à h^{-1} qui doit aussi appartenir à G_2. Cela nous impose d'avoir $(a', b', c', d', e', f') \in \mathbb{Z}^6$ où le sextuplet (a', b', c', d', e', f') est associé à h^{-1}. Comme les parties linéaires de h et h^{-1} sont inverses l'une de l'autre (il s'agit d'une propriété classique des applications affines : l'application réciproque d'une application affine bijective h est affine de partie linéaire l'application réciproque de la partie linéaire de h, [15], Th. 16), on obtient $MM' = I$ (où I désigne la matrice identité). Par suite $(\det M) \times (\det M') = 1$ et l'entier $\det M$ divise 1, donc $\Delta = \det M = \pm 1$.

III.4.a. • On a

$$\begin{cases} P_1\,(x, 0) \in \mathcal{S} \setminus \{O\} \;\Leftrightarrow\; x^2 + x = 0 \;\Leftrightarrow\; x = -1 \\ P_2\,(0, y) \in \mathcal{S} \setminus \{O\} \;\Leftrightarrow\; y^2 - y = 0 \;\Leftrightarrow\; y = 1 \end{cases}$$

donc $P_1\,(-1, 0)_{\mathcal{R}_0}$ et $P_2\,(0, 1)_{\mathcal{R}_0}$. Dans le repère $\mathcal{R}_0$, l'expression analytique de f_1 est

$$\begin{cases} x' = ax + by + c \\ y' = dx + ey + f \end{cases}$$

avec

$$\left\{\begin{array}{l} -\dfrac{1}{5} = -\dfrac{a}{5} + \dfrac{b}{5} + c \\ \dfrac{1}{5} = -\dfrac{d}{5} + \dfrac{e}{5} + f \\ -1 = c \\ 0 = f \\ 0 = -a + c \\ 0 = -d + f \end{array}\right. \quad \text{i.e.} \quad \left\{\begin{array}{l} b = 3 \\ e = 1 \\ c = -1 = a \\ f = 0 = d. \end{array}\right.$$

Ainsi

$$f_1 : \quad \left\{\begin{array}{l} x_1 = -x + 3y - 1 \\ y_1 = y. \end{array}\right.$$

De la même manière, si f_2 est décrit par les formules

$$\left\{\begin{array}{l} x' = ax + by + c \\ y' = dx + ey + f, \end{array}\right.$$

$$\left\{\begin{array}{l} -\dfrac{1}{5} = -\dfrac{a}{5} + \dfrac{b}{5} + c \\ \dfrac{1}{5} = -\dfrac{d}{5} + \dfrac{e}{5} + f \\ 0 = c \\ 1 = f \\ 0 = b + c \\ 0 = e + f \end{array}\right. \quad \text{i.e.} \quad \left\{\begin{array}{l} a = 1 \\ d = 3 \\ c = 0 = b \\ f = 1 = -e, \end{array}\right.$$

et

$$f_2 : \quad \left\{\begin{array}{l} x_2 = x \\ y_2 = 3x - y + 1. \end{array}\right.$$

Les formules de changement de repère entre $\mathcal{R}_0$ et $\mathcal{R}_1$ ont été trouvées à de la question III.1.c :

$$\left\{\begin{array}{l} X = \dfrac{\sqrt{5}+3}{2}\left(x + \dfrac{1}{5}\right) - \left(y - \dfrac{1}{5}\right) \\ Y = \dfrac{\sqrt{5}-3}{2}\left(x + \dfrac{1}{5}\right) + \left(y - \dfrac{1}{5}\right). \end{array}\right.$$

$$\left\{\begin{array}{l} x = \dfrac{\sqrt{5}}{5}X + \dfrac{\sqrt{5}}{5}Y - \dfrac{1}{5} \\ y = \dfrac{3\sqrt{5}-5}{10}X + \dfrac{3\sqrt{5}+5}{10}Y + \dfrac{1}{5}. \end{array}\right.$$

On a

$$\begin{aligned} X_1 &= \frac{\sqrt{5}+3}{2}\left(x_1+\frac{1}{5}\right)-\left(y_1-\frac{1}{5}\right) \\ &= \frac{\sqrt{5}+3}{2}\left(-x+3y-1+\frac{1}{5}\right)-\left(y-\frac{1}{5}\right) \\ &= -\frac{\sqrt{5}+3}{2}x+\frac{3\sqrt{5}+7}{2}y-\frac{2\sqrt{5}+5}{5} \\ &= -\frac{\sqrt{5}+3}{2}\left(\frac{\sqrt{5}}{5}X+\frac{\sqrt{5}}{5}Y-\frac{1}{5}\right) \\ &\qquad +\frac{3\sqrt{5}+7}{2}\left(\frac{3\sqrt{5}-5}{10}X+\frac{3\sqrt{5}+5}{10}Y+\frac{1}{5}\right)-\frac{5+2\sqrt{5}}{5} \\ &= \frac{7+3\sqrt{5}}{2}Y = \lambda Y. \end{aligned}$$

Des calculs du même genre donnent

$$Y_1 = \frac{7-3\sqrt{5}}{2}X = \frac{1}{\lambda}X \ ; \quad X_2 = Y \quad \text{et} \quad Y_2 = X.$$

• f_1 et f_2 sont des bijections du type $h_{1,\mu}$ défini en III.2.e (on a $f_1 = h_{1,\lambda}$ et $f_2 = h_{1,1}$), donc appartiennent à G_1. Ce sont des symétries, comme tous les éléments $h_{1,\mu}$ (voir III.2.e). Les expressions analytiques de f_1 et f_2 dans le repère $\mathcal{R}_0$ et la caractérisation obtenue en III.3.c (coefficients entiers et déterminant de la partie linéaire non nul) montrent que f_1 et f_2 appartiennent aussi à G_2. Donc $f_1,\ f_2 \in G_1 \cap G_2$.

III.4.b. Dans ce qui suit, on notera souvent $f_1 f_2$ au lieu de $f_1 \circ f_2$ pour simplifier. Comme f_1 et f_2 sont des symétries, elles sont involutives et l'on a $f_1^{-1} = f_1$ et $f_2^{-1} = f_2$. En particulier $(f_2 f_1)^{-1} = f_1 f_2$. Posons $\Lambda = \{f_1, f_2\}$.

Première méthode : De façon générale (voir § 5.3.2), le sous-groupe Γ engendré par Λ est $\Gamma = \{g_1^{\alpha_1}...g_m^{\alpha_m} \,/\, m \in \mathbb{N},\ \alpha_i \in \mathbb{Z},\ g_i \in \Lambda\}$. Comme f_1 et f_2 sont involutives, cela s'écrit $\Gamma = \{f_1^{\alpha_1} f_2^{\alpha_2}...f_m^{\alpha_m} \,/\, m \in \mathbb{N},\ \alpha_i \in \{0,1\}\}$, et les éléments de Γ seront de l'une des quatre formes suivantes :

(a) $f_1 f_2 f_1 ... f_2 f_1$, que l'on écrit $f_1 (f_2 f_1)^k = f_2 (f_2 f_1)^{k+1} = f_2 (f_1 f_2)^{-(k+1)}$,

(b) $f_1 f_2 f_1 ... f_1 f_2$, ce qui s'écrit $(f_1 f_2)^k$,

(c) $f_2 f_1 f_2 ... f_1 f_2$, ce qui s'écrit $f_2 (f_1 f_2)^k$,

(d) $f_2 f_1 f_2 ... f_2 f_1$, que l'on écrit $(f_2 f_1)^k$, ou encore $(f_1 f_2)^{-k}$.

On obtient bien $\Gamma = \left\{ (f_1 \circ f_2)^k \ / \, k \in \mathbb{Z} \right\} \cup \left\{ f_2 \circ (f_1 \circ f_2)^k \ / \, k \in \mathbb{Z} \right\}$.

Seconde méthode : On vérifie que

$$\Gamma = \left\{ (f_1 \circ f_2)^k \ / \, k \in \mathbb{Z} \right\} \cup \left\{ f_2 \circ (f_1 \circ f_2)^k \ / \, k \in \mathbb{Z} \right\}$$

est le sous-groupe engendré par f_1 et f_2 en retournant à la définition. On démontre donc les trois points suivants :

• Γ contient la paire $\Lambda = \{f_1, f_2\}$: c'est évident puisque $f_2 \circ (f_1 \circ f_2)^0 = f_2$ appartient à Γ, tout comme $f_1 = f_2 \circ (f_2 \circ f_1) = f_2 \circ (f_1 \circ f_2)^{-1}$.

• Γ est un sous-groupe de $\mathrm{GA}(\mathcal{P})$. C'est une partie non vide de $\mathrm{GA}(\mathcal{P})$ (elle contient f_1 et f_2). Elle est stable par inverse puisque pour tout $k \in \mathbb{Z}$,

$$\left((f_1 f_2)^k \right)^{-1} = (f_1 f_2)^{-k}$$

et

$$\left(f_2 \, (f_1 f_2)^k \right)^{-1} = (f_1 f_2)^{-k} f_2 = (f_2 f_1)^k f_2 \underset{\Game}{=} f_2 \, (f_1 f_2)^k . \quad (*)$$

Notons que l'égalité $\Game$ se vérifie en envisageant deux cas : si $k \in \mathbb{N}$, on écrit

$$(f_2 f_1)^k f_2 = (f_2 f_1)(f_2 f_1) \ldots (f_2 f_1) f_2 = f_2 \, (f_1 f_2) \ldots (f_1 f_2) = f_2 \, (f_1 f_2)^k$$

(ou bien l'on raisonne par récurrence sur k si l'on veut rester plus rigoureux). Si $k \in \mathbb{Z}_-$, on écrit

$$(f_2 f_1)^k f_2 = f_2 \, (f_1 f_2)^k \ \Leftrightarrow \ f_2 \, (f_1 f_2)^{-k} = (f_2 f_1)^{-k} f_2$$

et l'on est ramené au cas précédent (puisque $-k \in \mathbb{N}$).
Enfin Γ est stable par composition puisque pour tout $(k, m) \in \mathbb{Z}^2$,

$$\begin{aligned}
&(f_1 f_2)^k (f_1 f_2)^m = (f_1 f_2)^{k+m} \\
&(f_2 \, (f_1 f_2)^k)(f_2 \, (f_1 f_2)^m) = (f_2 \, (f_1 f_2)^k)(f_2 \, (f_1 f_2)^k)(f_1 f_2)^{m-k} \\
&\qquad = (f_1 f_2)^{m-k} \ \text{(en utilisant la relation } (*)) \\
&(f_1 f_2)^k (f_2 \, (f_1 f_2)^m) = f_2 (f_2 \, (f_1 f_2)^k)(f_2 \, (f_1 f_2)^m) \\
&\qquad = f_2 \, (f_1 f_2)^{m-k} \ \text{(en utilisant la relation précédente)} \\
&(f_2 \, (f_1 f_2)^k)(f_1 f_2)^m = f_2 \, (f_1 f_2)^{k+m}
\end{aligned}$$

• Si H est un sous-groupe contenant Λ, alors H contient toutes les composées $(f_1 \circ f_2)^k$ et $f_2 \circ (f_1 \circ f_2)^k$ (où $k \in \mathbb{Z}$) donc contient Γ.

III.4.c. • Considérons à nouveau l'homomorphisme de groupes

$$\begin{array}{rccc}
\Phi : & (\mathrm{GA}(\mathcal{P}), \circ) & \longrightarrow & (\mathrm{GL}_2(\mathbb{R}), \times) \\
& h & \longmapsto & \Phi(h)
\end{array}$$

qui à h associe la matrice de la partie linéaire de h dans la base $(\overrightarrow{u}, \overrightarrow{v})$. La restriction $\Phi_0 : (\mathrm{GA}_I(\mathcal{P}), \circ) \longrightarrow (\mathrm{GL}_2(\mathbb{R}), \times)$ de Φ au groupe $\mathrm{GA}_I(\mathcal{P})$ des bijections affines qui laissent le point I invariant ($\mathrm{GA}_I(\mathcal{P})$ est appelé "stabilisateur de I dans $\mathrm{GA}(\mathcal{P})$") est un isomorphisme de groupe (en effet, étant donné un automorphisme l de P, il existe une et une seule application affine de partie linéaire l et admettant I comme point invariant).
On a $G_1 \subset \mathrm{GA}_I(\mathcal{P})$ et $G_2 \subset \mathrm{GA}_I(\mathcal{P})$. Comme f_1 et f_2 appartiennent à $G_1 \cap G_2$, le sous-groupe Γ engendré par f_1 et f_2 sera inclus dans $\mathrm{GA}_I(\mathcal{P})$, et Γ pourra être considéré comme le sous-groupe de $\mathrm{GA}_I(\mathcal{P})$ engendré par f_1 et f_2. Comme Φ_0 est un isomorphisme, on peut affirmer que $\Phi_0(\Gamma)$ sera le sous-groupe Γ_1 de $\mathrm{GL}_2(\mathbb{R})$ engendré par $\Phi(f_1) = A_1$ et $\Phi(f_2) = A_2$.
On vient de prouver que Γ est isomorphe à Γ_1 et d'exhiber l'isomorphisme $\Phi_0|_\Gamma : \Gamma \longrightarrow \Gamma_1$.

- On a
$$A_1A_2 = \begin{pmatrix} 0 & \lambda \\ 1/\lambda & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \lambda & 0 \\ 0 & 1/\lambda \end{pmatrix}.$$

- Pour tout $k \in \mathbb{Z}$,
$$\Phi\left((f_1 \circ f_2)^k\right) = (A_1A_2)^k = \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix}$$

et
$$\begin{aligned} \Phi\left(f_2 \circ (f_1 \circ f_2)^k\right) &= A_2 (A_1A_2)^k \\ &= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix} = \begin{pmatrix} 0 & \lambda^{-k} \\ \lambda^k & 0 \end{pmatrix}, \end{aligned}$$

par conséquent
$$\Gamma_1 = \left\{ \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix} / k \in \mathbb{Z} \right\} \cup \left\{ \begin{pmatrix} 0 & \lambda^{-k} \\ \lambda^k & 0 \end{pmatrix} / k \in \mathbb{Z} \right\}.$$

- On sait que tout élément h de Γ s'écrit sous la forme (i) $(f_1 \circ f_2)^k$ ou (ii) $f_2 \circ (f_1 \circ f_2)^k$ (avec $k \in \mathbb{Z}$).

α) h ne peut pas s'écrire simultanément sous la forme (i) et (ii), autrement il existerait deux entiers relatifs k et m tels que $(f_1 \circ f_2)^k = f_2 \circ (f_1 \circ f_2)^m$, et l'on aurait $(A_1A_2)^k = A_2 (A_1A_2)^m$, soit
$$\begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix} = \begin{pmatrix} 0 & \lambda^{-m} \\ \lambda^m & 0 \end{pmatrix},$$

ce qui est impossible.

β) Si h s'écrit sous la forme $h = (f_1 \circ f_2)^k$, et si $h = (f_1 \circ f_2)^k = (f_1 \circ f_2)^m$, alors $(A_1A_2)^k = (A_1A_2)^m$ donc $\lambda^k = \lambda^m$. Cela impose d'avoir $k = m$, et prouve que l'écriture sous la forme (i) est unique.

γ) Si $h = f_2 \circ (f_1 \circ f_2)^k = f_2 \circ (f_1 \circ f_2)^m$, on obtient cette fois-ci l'égalité matricielle $A_2 (A_1A_2)^k = A_2 (A_1A_2)^m$ donc encore $\lambda^k = \lambda^m$, ce qui donne $k = m$.

L'écriture d'un élément de Γ donnée en III.4.b est donc unique.

III.4.d. Si un tel morphisme existe, il est parfaitement défini en posant, pour tout $k \in \mathbb{Z}$, $\phi\left((f_1 \circ f_2)^k\right) = (a_1a_2)^k$ et $\phi\left(f_2 \circ (f_1 \circ f_2)^k\right) = a_2 (a_1a_2)^k$. L'unicité de ϕ est donc assurée. Il reste à vérifier que ϕ, définie sur Γ par les formules ci-dessus, est bien un morphisme de groupe, autrement dit

$$\forall h_1, h_2 \in \Gamma \quad \phi (h_1 \circ h_2) = \phi (h_1) \phi (h_2) .$$

Il faut envisager quatre cas suivant que h_1 et h_2 soient du type (i) ou (ii). Vérifions seulement le cas où $h_1 = (f_1 \circ f_2)^k$ et $h_2 = f_2 \circ (f_1 \circ f_2)^m$, les autres cas se traitant de façon identique en utilisant les formules donnant les produits des éléments de Γ obtenus dans la seconde méthode proposée en III.4.b. On a

$$\begin{cases} \phi (h_1 \circ h_2) = \phi\left(f_2 (f_1f_2)^{m-k}\right) = a_2 (a_1a_2)^{m-k} \\ \phi (h_1) \phi (h_2) = (a_1a_2)^k a_2 (a_1a_2)^m \end{cases}$$

et l'on vérifie (comme en III.4.b, mais avec des a_i à la place des f_i) que

$$(a_1a_2)^k a_2 (a_1a_2)^m = a_2 (a_1a_2)^{m-k} .$$

III.5.a. Le groupe Γ, engendré par f_1 et f_2, laisse $\mathcal{S}$ stable si et seulement si $f_1 (\mathcal{S}) = \mathcal{S}$ et $f_2 (\mathcal{S}) = \mathcal{S}$. D'après III.4.a, les bijections f_i appartiennent à $G_1 \cap G_2$, donc vérifient $f_i (\mathcal{C}) = \mathcal{C}$ et $f_i (\mathcal{Z}) = \mathcal{Z}$. Comme $\mathcal{S} = \mathcal{C} \cap \mathcal{Z}$, on obtient bien $f_i (\mathcal{S}) = f_i (\mathcal{C} \cap \mathcal{Z}) = f_i (\mathcal{C}) \cap f_i (\mathcal{Z}) = \mathcal{C} \cap \mathcal{Z} = \mathcal{S}$.

La question III.4.a nous donne les formules analytiques définissant f_1 et f_2 dans $\mathcal{R}_0$:

$$f_1 : \begin{cases} x_1 = -x + 3y - 1 \\ y_1 = y. \end{cases} \quad \text{et} \quad f_2 : \begin{cases} x_2 = x \\ y_2 = 3x - y + 1, \end{cases}$$

d'où

$$f_1 \circ f_2 : \begin{cases} x' = 8x - 3y + 2 \\ y' = 3x - y + 1. \end{cases}$$

Ainsi, en identifiant points et coordonnées dans $\mathcal{R}_0$:

$$\begin{cases} M_1 = (f_1 \circ f_2) (O) = (2, 1)_{\mathcal{R}_0} \\ M_2 = (f_1 \circ f_2) (M_1) = (15, 6)_{\mathcal{R}_0} \\ M_3 = (f_1 \circ f_2) (M_2) = (104, 40)_{\mathcal{R}_0} . \end{cases}$$

On reconnaît les trois solutions de l'équation diophantienne (Σ_1) obtenues en II.2.c.

III.5.b. • En III.4.c nous avons obtenu la matrice de la partie linéaire de $(f_1 \circ f_2)^k$ dans la base $(\overrightarrow{u}, \overrightarrow{v})$:

$$\Phi\left((f_1 \circ f_2)^k\right) = (A_1 A_2)^k = \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix},$$

et III.1.c nous donne les formules de changement de repère de $\mathcal{R}_0 = (O, \overrightarrow{i}, \overrightarrow{j})$ vers $\mathcal{R}_1 = (I, \overrightarrow{u}, \overrightarrow{v})$:

$$\begin{cases} X = \frac{\sqrt{5}+3}{2}\left(x + \dfrac{1}{5}\right) - \left(y - \dfrac{1}{5}\right) \\ Y = \frac{\sqrt{5}-3}{2}\left(x + \dfrac{1}{5}\right) + \left(y - \dfrac{1}{5}\right) \end{cases} \text{ et } \begin{cases} x = \dfrac{\sqrt{5}}{5}X + \dfrac{\sqrt{5}}{5}Y - \dfrac{1}{5} \\ y = \dfrac{3\sqrt{5}-5}{10}X + \dfrac{3\sqrt{5}+5}{10}Y + \dfrac{1}{5}. \end{cases}$$

Donc $O = \left(\dfrac{\sqrt{5}+5}{10}, \dfrac{\sqrt{5}-5}{10}\right)_{\mathcal{R}_1}$, et $M_k = (f_1 \circ f_2)^k(O) = (X_k, Y_k)_{\mathcal{R}_1}$ avec

$$\begin{pmatrix} X_k \\ Y_k \end{pmatrix} = \begin{pmatrix} \lambda^k & 0 \\ 0 & \lambda^{-k} \end{pmatrix} \begin{pmatrix} \frac{\sqrt{5}+5}{10} \\ \frac{\sqrt{5}-5}{10} \end{pmatrix} = \begin{pmatrix} \frac{\sqrt{5}+5}{10}\lambda^k \\ \frac{\sqrt{5}-5}{10}\lambda^{-k} \end{pmatrix}.$$

Puis $M_k = (x_k, y_k)_{\mathcal{R}_0}$ avec

$$\begin{pmatrix} x_k \\ y_k \end{pmatrix} = \begin{pmatrix} \frac{1+\sqrt{5}}{10}\lambda^k + \frac{1-\sqrt{5}}{10}\lambda^{-k} - \frac{1}{5} \\ -\frac{1-\sqrt{5}}{10}\lambda^k - \frac{1+\sqrt{5}}{10}\lambda^{-k} + \frac{1}{5} \end{pmatrix}$$

• On constate que $x_{-k} = -y_k$ et $y_{-k} = -x_k$, de sorte que M_k se déduise de M_{-k} par la réflexion de base la seconde bissectrice (d'équation $y = -x$ dans $\mathcal{R}_0$).

Remarque : La rédaction précédente signale rapidement que l'on est en présence d'une réflexion par rapport la seconde bissectrice. Pour le voir au brouillon, on peut bien sûr faire un dessin. On peut aussi noter que l'application affine $(x, y) \mapsto (-y, -x)$ est involutive et que sa partie linéaire conserve manifestement la norme. Il s'agit donc d'une symétrie affine orthogonale par rapport au sous-espace affine de ses points invariants. Ce sous-espace admet l'équation $y = -x$, c'est donc une droite, et l'on peut affirmer que l'application $(x, y) \mapsto (-y, -x)$ est la réflexion par rapport à cette droite.

III.5.c. • Montrons que ϕ_1 et ϕ_2 sont bijectives et calculons les applications réciproques.

Le discriminant réduit du trinôme $5x^2+2x+1$ est -4, donc ce trinôme reste strictement positif pour tout $x \in \mathbb{R}$. Les fonctions ϕ_1 et ϕ_2 sont donc parfaitement définies et continûment dérivable sur $\mathbb{R}$ en entier. A partir de là, on peut choisir l'une des méthodes suivantes.

Première méthode : On s'intéresse à ϕ_1 et ϕ_2 successivement et l'on retourne à la définition d'une bijection. Je ne traiterai ici que le cas de ϕ_1, l'autre cas se résolvant de façon identique.
Montrer que ϕ_1 est une bijection de $\mathbb{R}$ dans $\mathbb{R}$ revient à prouver que l'équation $\phi_1(x) = y$ admet une unique solution x quel que soit le réel y donné. On résout donc :

$$1+3x-\sqrt{1+2x+5x^2} = 2y \quad (*)$$

On a

$$\begin{aligned}(*) &\Leftrightarrow \sqrt{1+2x+5x^2} = 1+3x-2y \\ &\Leftrightarrow \begin{cases} 1+2x+5x^2 = (1+3x-2y)^2 & (1) \\ 1+3x-2y \geq 0 & (2) \end{cases}\end{aligned}$$

L'équation (1) s'écrit $x^2+(1-3y)\,x+y^2-y=0$, et son discriminant est $5y^2-2y+1$. Elle admet donc les solutions

$$x = \frac{3y-1\pm\sqrt{1-2y+5y^2}}{2}.$$

L'inéquation (2) permet d'éliminer l'une de ces solutions pour n'en retenir qu'une. En effet

$$1+3\frac{3y-1-\sqrt{1-2y+5y^2}}{2}-2y \geq 0$$

équivaut successivement à

$$4y \leq 2+9y-3-3\sqrt{1-2y+5y^2}$$

$$3\sqrt{1-2y+5y^2} \leq 5y-1$$

ou encore à

$$9\left(1-2y+5y^2\right) \leq (5y-1)^2$$

en supposant $y \geq 1/5$. Pas d'espoir cependant, car cette dernière inéquation s'écrit $5y^2-2y+2 \leq 0$, ce qui n'est vérifié par aucun y, le trinôme du premier membre étant de discriminant réduit -9 strictement négatif, et restant ainsi strictement positif pour tout y.

Pour voir si l'on peut retenir l'autre solution, il faut maintenant vérifier que (2) est satisfait pour tout y, c'est-à-dire

$$\forall y \in \mathbb{R} \quad 1 + 3\frac{3y - 1 + \sqrt{1 - 2y + 5y^2}}{2} - 2y \geq 0$$

L'inéquation qui nous intéresse s'écrit successivement

$$4y \leq 2 + 9y - 3 + 3\sqrt{1 - 2y + 5y^2}$$
$$1 - 5y \leq 3\sqrt{1 - 2y + 5y^2}.$$

Cette inéquation est trivialement vérifiée si $y \geq 1/5$ car un radical est toujours positif. Si $y < 1/5$, elle équivaut à $(1 - 5y)^2 \leq 9\left(1 - 2y + 5y^2\right)$, ce qui s'écrit encore $5y^2 - 2y + 2 \geq 0$, et tout va bien puisque le trinôme du premier membre reste strictement positif pour tout y.

En conclusion, l'équation $(*)$ admet une unique solution quel que soit y appartenant à $\mathbb{R}$, et cette solution est

$$x = \frac{3y - 1 + \sqrt{1 - 2y + 5y^2}}{2}.$$

$\phi_1 : \mathbb{R} \to \mathbb{R}$ est donc bijective, et

$$\forall y \in \mathbb{R} \quad \phi_1^{-1}(y) = \frac{3y - 1 + \sqrt{1 - 2y + 5y^2}}{2}.$$

Deuxième méthode : On utilise les dérivées des fonctions ϕ_1 et ϕ_2, et le fait que $\phi_1(x) < \phi_2(x)$ pour tout réel x. On trouve

$$\phi_1'(x) = \frac{3\sqrt{1 + 2x + 5x^2} - 1 - 5x}{2\sqrt{1 + 2x + 5x^2}} \text{ et } \phi_2'(x) = \frac{3\sqrt{1 + 2x + 5x^2} + 1 + 5x}{2\sqrt{1 + 2x + 5x^2}}.$$

Si $\phi_1'(x) = 0$ ou $\phi_2'(x) = 0$, alors $9\left(1 + 2x + 5x^2\right) = (1 + 5x)^2$, c'est-à-dire $5x^2 + 2x + 2 = 0$. Mais le trinôme $5x^2 + 2x + 2$ n'admet pas de racine réelle. On peut donc affirmer que $\phi_1'(x)$ et $\phi_2'(x)$ ne s'annulent jamais et (en utilisant la continuité de ces dérivées et le Théorème des valeurs intermédiaires) restent ou bien strictement positifs, ou bien strictement négatifs, lorsque x décrit $\mathbb{R}$. Comme $\phi_1'(0) = 1$ et $\phi_2'(0) = 2$, les dérivées ϕ_1' et ϕ_2' seront strictement positives sur $\mathbb{R}$, et les fonctions ϕ_1 et ϕ_2 seront strictement croissantes de $\mathbb{R}$ dans $\mathbb{R}$. On vérifie facilement que $\lim_{x\to\pm\infty} \phi_i(x) = \pm\infty$ (pour tout i). Par exemple, si $x > 0$,

$$\phi_1(x) = \frac{1}{2}\left(1 + 3x - \sqrt{1 + 2x + 5x^2}\right) = \frac{x}{2}\left(\frac{1}{x} + 3 - \sqrt{\frac{1}{x^2} + \frac{2}{x} + 5}\right)$$

nous présente $\phi_1(x)$ sous la forme d'un produit dont le premier facteur tend vers $+\infty$ (quand $x \to +\infty$) et dont le second facteur tend vers $3 - \sqrt{5} > 0$. On obtient bien $\lim_{x\to+\infty} \phi_1(x) = +\infty$. Les autres cas se traitent de la même façon.
On peut maintenant affirmer que ϕ_1 et ϕ_2 sont des bijections strictement croissantes de $\mathbb{R}$ sur $\mathbb{R}$.

Comme

$$\left.\begin{array}{c}\phi_1(x) = y \\ \text{ou} \\ \phi_2(x) = y\end{array}\right\} \Rightarrow\ 1 + 2x + 5x^2 = (1 + 3x - 2y)^2,$$

pour tout $y \in \mathbb{R}$, les réels $\phi_1^{-1}(y)$ et $\phi_2^{-1}(y)$ sont des solutions de l'équation du second degré en x

$$1 + 2x + 5x^2 = (1 + 3x - 2y)^2 \quad (1)$$

que l'on résout comme dans la première solution pour obtenir

$$x = \frac{3y - 1 \pm \sqrt{1 - 2y + 5y^2}}{2}.$$

On note que $\phi_1(x) < \phi_2(x)$ pour tout x. La croissance des fonctions ϕ_i et donc des ϕ_i^{-1} permet alors d'écrire

$$\phi_1(x) < \phi_2(x)\ \Rightarrow\ x < \phi_1^{-1}(\phi_2(x))\ \Rightarrow\ \phi_2^{-1}(y) < \phi_1^{-1}(y),$$

et de conclure à $\phi_2^{-1}(y) < \phi_1^{-1}(y)$ pour tout y. Les réels $\phi_1^{-1}(y)$ et $\phi_2^{-1}(y)$ sont donc les deux solutions distinctes de l'équation du second degré (1), dans l'ordre $\phi_2^{-1}(y) < \phi_1^{-1}(y)$, soit

$$\phi_1^{-1}(y) = \frac{3y - 1 + \sqrt{1 - 2y + 5y^2}}{2} \quad \text{et} \quad \phi_2^{-1}(y) = \frac{3y - 1 - \sqrt{1 - 2y + 5y^2}}{2}.$$

- On a

$$\begin{aligned} M(x,y)_{\mathcal{R}_0} \in \mathcal{C} &\Leftrightarrow y^2 - (3x+1)\,y + x^2 + x = 0 \\ &\Leftrightarrow y = \frac{1}{2}\left(1 + 3x \pm \sqrt{1 + 2x + 5x^2}\right) \\ &\Leftrightarrow M \in \mathcal{C}_1 \cup \mathcal{C}_2. \end{aligned}$$

On a aussi $\mathcal{C}_1 \cap \mathcal{C}_2 = \varnothing$ puisque $\phi_1(x) < \phi_2(x)$ pour tout $x \in \mathbb{R}$. Les graphes $\mathcal{C}_1$ et $\mathcal{C}_2$ n'étant pas vides, on peut affirmer que $\mathcal{C}_1$ et $\mathcal{C}_2$ forment une partition de $\mathcal{C}$.

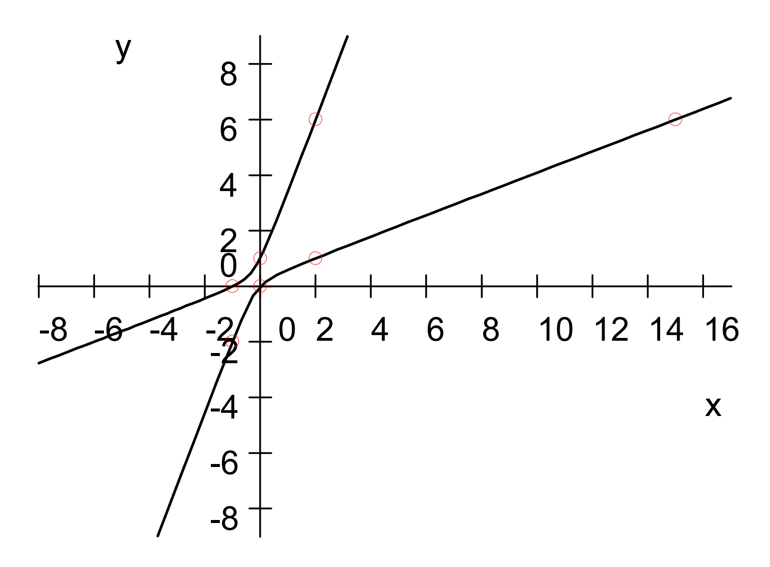


FIG. 5.8 – 7 points à coordonnées entières sur $\mathcal{C}$

• On a déjà $M_0\,(0,0)_{\mathcal{R}_0}$; $M_1\,(2,1)_{\mathcal{R}_0}$ et $M_2\,(15,6)_{\mathcal{R}_0}$ d'après III.4.a. La question III.5.b montre que M_{-1} est le symétrique de M_1 par rapport à la seconde bissectrice, soit $M_{-1}\,(-1,-2)_{\mathcal{R}_0}$. Enfin $N_k = f_2\,(M_k)$ avec

$$f_2 : \begin{cases} x_2 = x \\ y_2 = 3x - y + 1, \end{cases}$$

donc $N_{-1}\,(-1,0)_{\mathcal{R}_0}$, $N_0\,(0,1)_{\mathcal{R}_0}$ et $N_1\,(2,6)_{\mathcal{R}_0}$. La FIG. 5.8 représente ces 7 points à coordonnées entières sur l'hyperbole $\mathcal{C}$.

III.5.d. • L'application f_1 est bijective et laisse $\mathcal{C}$ invariante, donc

$$\mathcal{C} = \mathcal{C}_1 \cup \mathcal{C}_2 \;\Rightarrow\; f_1\,(\mathcal{C}) = \mathcal{C} = f_1\,(\mathcal{C}_1) \cup f_1\,(\mathcal{C}_2)$$

et $f_1\,(\mathcal{C}_1)$, $f_1\,(\mathcal{C}_2)$ forment une partition de $\mathcal{C}$. Montrer que $f_1\,(\mathcal{C}_1) = \mathcal{C}_2$ et $f_1\,(\mathcal{C}_2) = \mathcal{C}_1$ revient donc à montrer que $f_1\,(\mathcal{C}_1) \subset \mathcal{C}_2$ et $f_1\,(\mathcal{C}_2) \subset \mathcal{C}_1$.
$\mathcal{C}_1$ et $\mathcal{C}_2$ sont les branches de l'hyperbole $\mathcal{C}$. Ce sont des parties connexes par arcs (par exemple $\mathcal{C}_1$ est connexe par arcs comme l'image du connexe par arcs $\mathbb{R}$ par l'application continue $x \mapsto (x, \phi_1\,(x))$), et puisque f_1 est continue,

l'image $f_1(\mathcal{C}_1)$ sera connexe par arcs. Par suite

$$\begin{aligned} M \in \mathcal{C}_1 &\Rightarrow (\text{Il existe un chemin continu joignant } O \text{ à } M \text{ et inclus dans } \mathcal{C}_1) \\ &\Rightarrow \left(\begin{array}{l} \text{Il existe un chemin continu joignant } f_1(O) = N_{-1} \\ \text{à } f_1(M) \text{ et restant dans } f_1(\mathcal{C}_1) \end{array} \right) \\ &\Rightarrow \left(\begin{array}{l} f_1(M) \text{ appartient à la composante} \\ \text{connexe de } N_{-1} \text{ dans } \mathcal{C}, \text{ i.e. } \mathcal{C}_2 \end{array} \right) \\ &\Rightarrow f_1(M) \in \mathcal{C}_2. \end{aligned}$$

On a prouvé l'inclusion $f_1(\mathcal{C}_1) \subset \mathcal{C}_2$, et l'on peut conclure à $f_1(\mathcal{C}_1) = \mathcal{C}_2$. On raisonnerait de même avec f_2.

• On en déduit $(f_1 \circ f_2)(\mathcal{C}_1) = f_1(f_2(\mathcal{C}_1)) = f_1(\mathcal{C}_2) = \mathcal{C}_1$, de sorte que $\mathcal{C}_1$ soit globalement invariante par $f_1 \circ f_2$. On montrerait de la même façon que $(f_1 \circ f_2)(\mathcal{C}_2) = \mathcal{C}_2$.

• Le point O appartient à $\mathcal{C}_1$ qui est invariante par $f_1 \circ f_2$, donc tous les points $M_k = (f_1 \circ f_2)^k(O)$ appartiennent à $\mathcal{C}_1$. Les points $N_k = f_2(M_k)$ appartiendront alors tous à $\mathcal{C}_2$.

IV.1.a. • Comme $P \in \mathcal{C}_1$, et comme $f_1 \circ f_2$ laisse $\mathcal{C}_1$ invariante, tous les points P_i appartiendront à $\mathcal{C}_1$, et l'on aura $\beta_i = \phi_1(\alpha_i)$.

• On a $P_{i+1} = (f_1 \circ f_2)^{-1}(P_i) = f_2(f_1(P_i))$, et les formules analytiques (obtenues en III.4.a) sont :

$$f_1 : \left\{ \begin{array}{l} x_1 = -x + 3y - 1 \\ y_1 = y. \end{array} \right. \quad \text{et} \quad f_2 : \left\{ \begin{array}{l} x_2 = x \\ y_2 = 3x - y + 1. \end{array} \right.$$

On remarque que f_1 conserve l'ordonnée d'un point, tandis que f_2 conserve l'abscisse d'un point. Donc

$$P_i = \begin{pmatrix} \alpha_i \\ \beta_i \end{pmatrix} = \begin{pmatrix} \alpha_i \\ \phi_1(\alpha_i) \end{pmatrix} \in \mathcal{C}_1,$$

$$f_1(P_i) = \begin{pmatrix} \phi_2^{-1}(\phi_1(\alpha_i)) \\ \phi_1(\alpha_i) \end{pmatrix} \in \mathcal{C}_2,$$

et

$$P_{i+1} = f_2(f_1(P_i)) = \begin{pmatrix} \phi_2^{-1}(\phi_1(\alpha_i)) \\ \phi_1\left(\phi_2^{-1}(\phi_1(\alpha_i))\right) \end{pmatrix} \in \mathcal{C}_1.$$

On obtient bien $\alpha_{i+1} = \phi_2^{-1} \circ \phi_1(\alpha_i)$.

IV.1.b. On a

$$\alpha_{i+1} < \alpha_i \;\Leftrightarrow\; \phi_2^{-1} \circ \phi_1(\alpha_i) < \alpha_i \;\Leftrightarrow\; \phi_1(\alpha_i) < \phi_2(\alpha_i)$$

et la dernière inégalité écrite est toujours vraie, puisque

$$\forall x \in \mathbb{R} \qquad \phi_1(x) \leq x < \phi_2(x).$$

Montrons par exemple que $\phi_1(x) \leq x$ pour tout x. On a

$$\phi_1(x) \leq x \iff x + 1 \leq \sqrt{2x + 5x^2 + 1}$$

et l'inégalité $x + 1 \leq \sqrt{2x + 5x^2 + 1}$ est triviale quand $x \leq -1$ (le membre de gauche étant négatif, et celui de droite positif). Si $x > -1$, on écrit

$$x + 1 \leq \sqrt{2x + 5x^2 + 1} \iff (x+1)^2 \leq 2x + 5x^2 + 1 \Leftrightarrow 0 \leq 4x^2$$

et l'inégalité est toujours vraie.
On peut donc affirmer que la suite $(\alpha_i)_{i\geq 0}$ est strictement décroissante. Si elle était minorée, elle convergerait vers une limite finie l. En passant à la limite dans l'égalité $\alpha_{i+1} = \phi_2^{-1} \circ \phi_1(\alpha_i)$ (ϕ_1 et ϕ_2 sont bien continues), on obtiendrait $\phi_1(l) = \phi_2(l)$ et le point de coordonnées $(l, \phi_1(l))$ appartiendrait à $\mathcal{C}_1 \cap \mathcal{C}_2$, ce qui est absurde car $\mathcal{C}_1 \cap \mathcal{C}_2 = \varnothing$ (III.5.c). Ainsi $\lim_{i\to+\infty} \alpha_i = -\infty$, et $]-\infty, n[= \bigsqcup_{i=1}^{+\infty} [\alpha_i \alpha_{i-1}[$. Comme $n > 0$, il existera une unique indice $k \geq 1$ tel que $\alpha_k \leq 0 < \alpha_{k-1}$.

Remarque : On peut aussi poser $k = \operatorname{Min}\{i \in \mathbb{N} \,/\, \alpha_i \leq 0\}$. Un tel minimum existe puisque la partie $\{i \in \mathbb{N} \,/\, \alpha_i \leq 0\}$ n'est pas vide (car $\lim_{i\to+\infty} \alpha_i = -\infty$) et incluse dans $\mathbb{N}$ (qui est un ensemble bien ordonné). Bien entendu $k \geq 1$ car $\alpha_0 = n$ est strictement positif par hypothèse.

IV.1.c. Supposons par l'absurde que $\alpha_k < 0$. Alors

$$\alpha_{k-1} = \phi_1^{-1} \circ \phi_2(\alpha_k) < \phi_1^{-1} \circ \phi_2(0) = 2$$

et l'abscisse α_{k-1} de P_{k-1} vérifie $0 < \alpha_{k-1} < 2$. On sait que f_1 et f_2 appartiennent à $G_1 \cap G_2$, c'est-à dire laissent invariantes $\mathcal{C}$ et $\mathcal{Z}$, donc aussi $\mathcal{S} = \mathcal{C} \cap \mathcal{Z}$. Puisque $P_0 = P \in \mathcal{S}$, on en déduit que $P_i = (f_1 \circ f_2)^{-i}(P) \in \mathcal{S}$ pour tout i. Alors P_{k-1} devrait être un point de $\mathcal{S}$ de coordonnées entières et d'abscisse α_{k-1} dans $]0, 2[$, c'est-à-dire $\alpha_{k-1} = 1$. C'est impossible, car en faisant $n = 1$ dans

$$n^2 + p^2 - 3np + n - p = 0,$$

on obtient $p^2 - 4p + 1 = 0$ qui n'admet aucune solution entière. Ainsi $\alpha_k = 0$, $\beta_k = \phi_1(\alpha_k) = \phi_1(0) = 0$ et $P_k = O$. On en déduit aussi

$$P = (f_1 \circ f_2)^k (P_k) = (f_1 \circ f_2)^k (O) = M_k.$$

Conclusion : On vient de prouver que $(\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\} = \{M_k \,/\, k\in\mathbb{N}^*\}$. Pour faire le point, j'écrirai :

$$P\in\mathcal{S} \quad\Leftrightarrow\quad \begin{cases} P=O \\ \quad\text{ou} \\ P\in(\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\} \Leftrightarrow P\in\{M_k\,/\,k\in\mathbb{N}^*\}\,. \\ \quad\text{ou} \\ P\in(\mathcal{S}\cap\mathcal{C}_2)\setminus\{O\} \end{cases}$$

IV.1.d. On a

$$(n,p) \text{ solution de } (\Sigma_1) \Leftrightarrow \begin{cases} (n,p)\in\mathbb{Z}^2 \\ 2\le p+1\le n \\ n^2+p^2-3np+n-p=0 \end{cases}$$
$$\Rightarrow \begin{cases} (n,p)\in\mathcal{S}\cap\mathcal{C} \\ n\ge 2 \end{cases} \Rightarrow (n,p)\in(\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\}\,.$$

La réciproque est vraie. Si $(n,p)\in(\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\}$, on a bien évidemment $n^2+p^2-3np+n-p=0$ et $n\ge 2$, mais il reste à vérifier que $2\le p+1\le n$. Il existe $k\in\mathbb{N}^*$ tel que $(n,p)=(\alpha_k,\beta_k)$, et l'on montre (comme en IV.1.b) que $\beta_k=\phi_1(\alpha_k)\le\alpha_k$. Mieux, comme $M_k\ne O$, on a $\beta_k=\phi_1(\alpha_k)<\alpha_k$ (même preuve qu'en IV.1.b, ou visualisation graphique : la représentation graphique de ϕ_1 est strictement sous la première bissectrice sauf pour l'abscisse 0), donc $\beta_k+1\le\alpha_k$. Par ailleurs $1\le\beta_k$ (puisque aucun point de $\mathcal{S}\cap\mathcal{C}_1$ n'a une abscisse strictement comprise entre 0 et 2, que $M_1\,(2,1)_{\mathcal{R}_0}$ est le premier point de $(\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\}$ obtenu et d'abscisse >0, qu'il est d'ordonnée 1, et que ϕ_1 est croissante sur $\mathbb{R}$).
Finalement $2\le\beta_k+1\le\alpha_k$ et l'on peut conclure :

L'ensemble des solutions de (Σ_1) est $(\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\}=\{M_k\,/\,k\in\mathbb{N}^*\}$.

IV.2.a. On a

$$n^2+p^2-3np+n-p=0 \Rightarrow (-p)^2+(-n)^2-3(-p)(-n)+(-p)-(-n)=0$$

donc

$$P\,(n,p)_{\mathcal{R}_0}\in\mathcal{S} \quad\Rightarrow\quad P'\,(-p,-n)_{\mathcal{R}_0}\in\mathcal{S}.$$

Comme $\phi_1(x)\le x<\phi_2(x)$ pour tout réel x (IV.1.b), on en déduit

$$\left(P\,(n,p)_{\mathcal{R}_0}\in\mathcal{C}_1 \text{ et } n<0\right) \Rightarrow p<n$$
$$\Rightarrow -n<-p \;\Rightarrow\; P'\,(-p,-n)_{\mathcal{R}_0}\in\mathcal{C}_1.$$

IV.2.b. La question précédente et la question IV.1.d permettent d'écrire

$$P'(-p,-n)_{\mathcal{R}_0} \in (\mathcal{S}\cap\mathcal{C}_1)\setminus\{O\} = \{M_k \,/\, k\in\mathbb{N}^*\},$$

de sorte qu'il existe $l\in\mathbb{N}^*$ tel que $P' = M_l$. En prenant les symétriques de ces points par rapport à la seconde bissectrice, et en utilisant III.5.b, on trouve $P = M_{-l}$ avec $-l < 0$.

IV.3. On a

$$\left.\begin{array}{l} P\in\mathcal{S} \;\Rightarrow\; f_2(P)\in\mathcal{S} \\ P\in\mathcal{C}_2 \;\Rightarrow\; f_2(P)\in\mathcal{C}_1 \end{array}\right\} \Rightarrow\; f_2(P)\in\mathcal{S}\cap\mathcal{C}_1,$$

ce qui nous incite à envisager trois cas :

▷ Si $f_2(P) = O$, alors $P = f_2(O) = (0,1)_{\mathcal{R}_0} = N_0$.

▷ Si $P(n,p)_{\mathcal{R}_0}$ est d'abscisse $n<0$, comme

$$f_2 : \begin{cases} x_2 = x \\ y_2 = 3x - y + 1, \end{cases}$$

$f_2(P)$ sera aussi d'abscisse <0. Comme $f_2(P)$ appartient à $\mathcal{S}\cap\mathcal{C}_1$, on peut appliquer IV.2 et en déduire l'existence d'un entier $k<0$ tel que $f_2(P) = M_k$. Par suite $P = f_2(M_k) = N_k$.

▷ Si $P(n,p)_{\mathcal{R}_0}$ est d'abscisse $n>0$, $f_2(P)$ aussi et l'on applique IV.1 : il existe $k\in\mathbb{N}^*$ tel que $f_2(P) = M_k$. On conclut comme précédemment : $P = f_2(M_k) = N_k$.

5.3 Compléments

5.3.1 Image d'une conique par une bijection affine

A titre d'entraînement, démontrons que l'image d'une conique par une bijection affine est une conique de même type (une telle question peut être posée à l'écrit comme à l'oral du concours, et il est alors bon de l'avoir rencontrée pendant sa préparation !). Avant d'entrer dans le vif du sujet, et pour bien comprendre la situation, nous devons nous souvenir de quelques points concernant les coniques.
Tout d'abord, il faut rappeler qu'une conique $\mathcal{C}$ peut être définie comme l'ensemble des points du plan dont les coordonnées (x,y) (dans un repère affine donné) vérifient une équation du type $P(x,y) = 0$ où

$$P(x,y) = ax^2 + by^2 + cxy + dx + ey + f = q(x,y) + g(x,y)$$

est un polynôme de degré 2 à deux variables x et y, et à coefficients réels. Dans ce polynôme, on distingue une partie quadratique $q(x,y) = ax^2 + by^2 + cxy$, et une partie affine $g(x,y) = dx + ey + f$.

- A partir de là, la première chose à vérifier est que cette définition a un sens, autrement dit qu'elle ne dépend pas du repère choisi. On vérifie qu'un changement de repère affine "transforme" une équation $P(x,y) = 0$, où P est un polynôme de degré 2 en x et y, en une autre équation $Q(x',y') = 0$ où Q est encore un polynôme de degré 2 en x' et y' (où x' et y' désignent les nouvelles coordonnées).

- La seconde chose à savoir, c'est que l'on définit ainsi des coniques "au sens large", c'est-à-dire des coniques "non dégénérées" (des paraboles, des hyperboles ou des ellipses qui peuvent être définies autrement, par exemple en utilisant un foyer et une directrice ; ou des cercles) et d'autres coniques, dites "dégénérées", qui ne sont autre que l'ensemble vide $\varnothing$, une droite, ou la réunion de deux droites (concourantes ou parallèles).

- Troisièmement, c'est la réduction de la partie quadratique $q(x,y)$ de $P(x,y)$ qui permet d'obtenir une équation réduite de $\mathcal{C}$ et de distinguer tous les cas possibles. Un premier classement consiste alors à définir des coniques de "type ellipse", de "type parabole" ou de "type hyperbole", suivant le signe du produit $\lambda\mu$ des valeurs propres λ et μ de la matrice

$$M = \begin{pmatrix} a & c/2 \\ c/2 & b \end{pmatrix}$$

de la forme quadratique q. Les trois points que l'on vient de rappeler sont détaillés dans les Sections 22.1.1 et 22.1.2 de [15].

On peut maintenant prouver :

> *Résultat 1* : L'image d'une conique (dégénérée ou non) par une bijection affine est une conique.

Preuve : L'équation $P(x,y) = 0$ d'une conique $\mathcal{C}$ dans un repère $(O, \overrightarrow{i}, \overrightarrow{j})$ s'écrit ${}^tXMX + NX + f = 0$ où $X = {}^t(x,y)$ et où N représente la matrice-ligne $\begin{pmatrix} d & e \end{pmatrix}$. Par ailleurs, une bijection affine h transforme un point de coordonnées (x,y) en un point de coordonnées (x',y') telles que

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} u & w \\ v & t \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \xi \\ \zeta \end{pmatrix},$$

où $T = \begin{pmatrix} u & w \\ v & t \end{pmatrix}$ désigne la matrice (inversible) de la partie linéaire de h dans la base $(\overrightarrow{i}, \overrightarrow{j})$.

Posons $A = {}^t(\xi, \zeta)$ et notons $X' = {}^t(x', y')$ le vecteur-colonne des coordonnées d'un point image de $M(x, y)$ par h. Notons aussi $W = T^{-1}$ l'inverse de la matrice M. On obtient $X' = TX + A$, soit $X = WX' - WA$, et une équation de $h(\mathcal{C})$ sera

$${}^t\left(WX' - WA\right) M \left(WX' - WA\right) + N \left(WX' - WA\right) + f = 0. \quad (\Diamond)$$

La partie quadratique de cette équation est ${}^tX'\left({}^tWMW\right)X'$. La matrice réelle symétrique ${}^tWMW$ n'est pas nulle (car $M \neq 0$) donc le premier membre de l'équation $(\Diamond)$ est encore un polynôme de degré 2 en x', y', et $h(\mathcal{C})$ est une conique (dégénérée ou non). ■

En fait, on a mieux :

Résultat 2 : L'image d'une conique (dégénérée ou non) par une bijection affine est une conique du même type.

Preuve : Avec les notations de la preuve précédente, la matrice ${}^tWMW$ est réelle symétrique, donc diagonalisable dans le groupe orthogonal, et à ce titre, admet deux valeurs propres réelles λ' et μ' éventuellement confondues. On peut alors écrire

$$\lambda'\mu' = \det\left({}^tWMW\right) = (\det W)^2 \times \det M = (\det W)^2 \times \lambda\mu,$$

de sorte que les produits $\lambda\mu$ et $\lambda'\mu'$ s'annulent simultanément, et sont de même signe s'ils ne sont pas nuls. Les coniques $\mathcal{C}$ et $h(\mathcal{C})$ sont donc bien de même type. ■

On peut encore améliorer ce dernier résultat :

Résultat 3 : Par une bijection affine, l'image :

a) de l'ensemble vide est l'ensemble vide,

b) d'une droite est une droite,

c) de la réunion de deux droites sécantes (resp. parallèles) est une réunion de deux droites sécantes (resp. parallèles),

d) d'une ellipse ou d'un cercle (éventuellement réduit à une point) est une ellipse ou un cercle (éventuellement réduit à une point) *[suivant les définitions que l'on choisit, un cercle peut être considéré comme une ellipse "particulière", et dans ce cas l'énoncé précédent se simplifie]*,

e) d'une hyperbole est une hyperbole,

f) d'une parabole est une parabole.

Preuve : Les assertions a), b) et c) sont des conséquences directes des propriétés des bijections affines : celles-ci transforment toujours une droite en une droite, et deux droites sécantes (resp. parallèles) en deux droites sécantes (resp. parallèles).
Considérons maintenant le cas où la conique $\mathcal{C}$ n'est pas dégénérée. La conique $h(\mathcal{C})$ ne peut pas alors être dégénérée (sinon h^{-1}, affine bijective, transformerait l'ensemble vide, ou une droite, ou une réunion de deux droites en une conique non dégénérée $\mathcal{C}$, ce qui est impossible d'après a), b) et c)).
Cette remarque faite, nous disons qu'il est facile de connaître la nature d'une conique non dégénérée en ne s'intéressant qu'à certaines de ses propriétés. Dans ce qui suit, pour simplifier, nous supposerons qu'une cercle est une ellipse particulière.
Parmi les trois coniques non dégénérées possibles, l'ellipse est la seule conique a être bornée. Or une bijection affine h transforme une partie bornée du plan en une autre partie bornée. On peut donc affirmer que l'image d'une ellipse par h est encore une ellipse, et cela prouve l'assertion d).
Une parabole et une hyperbole ne sont pas bornées, mais une hyperbole possède deux branches, autrement dit deux composantes connexes. Une bijection affine étant une continue, elle transforme un connexe en un connexe, donc transforme une hyperbole formée de deux composantes connexes, en une conique non dégénérée formée de deux composantes connexes, c'est-à-dire en une hyperbole.
Le raisonnement est encore valide si l'on s'intéresse à l'image d'une parabole : celle-ci devra être une conique non dégénérée et connexe, c'est-à-dire encore une parabole. ■

5.3.2 Eléments d'un sous-groupe engendré par une partie

Il est important de connaître la forme générale des éléments du sous-groupe engendré par une partie non vide Λ d'un groupe G noté multiplicativement. C'est utile pour l'écrit comme pour l'oral d'un concours.
Soit $(G,.)$ un groupe noté multiplicativement. Soit Λ une partie non vide de G. On montre que le sous-groupe $<\Lambda>$ de G engendré par Λ est

$$<\Lambda>=\{a_1^{\alpha_1}...\,a_m^{\alpha_m}\,/\,m\in\mathbb{N},\ \alpha_i\in\mathbb{Z},\ a_i\in\Lambda\}$$

en retournant à la définition d'un sous-groupe engendré. Montrer que l'ensemble $B=\{a_1^{\alpha_1}...\,a_m^{\alpha_m}\,/\,m\in\mathbb{N},\ \alpha_i\in\mathbb{Z},\ a_i\in\Lambda\}$ est égal au sous-groupe de G engendré par Λ revient à montrer que B est le plus petit sous-groupe de G contenant Λ (au sens de l'inclusion).

▶ Montrons que B est un sous-groupe de G. Tout d'abord B n'est pas vide, puisqu'il contient l'élément neutre e de G (en effet, $e=a^0$ où a désigne un

élément quelconque de Λ). Ensuite, si $x = a_1^{\alpha_1}...a_m^{\alpha_m}$ et $y = b_1^{\beta_1}...b_s^{\beta_s}$ désignent deux éléments quelconques de B, le produit

$$xy^{-1} = a_1^{\alpha_1}...\,a_m^{\alpha_m}.b_s^{-\beta_s}...\,b_1^{-\beta_1}$$

est encore de la forme voulue, donc appartient à B.

▶ L'ensemble B contient Λ : si $a \in \Lambda$, l'élément $a = a^1$ appartient à B par définition de B.

▶ Il reste à montrer que tout sous-groupe H de G qui contient Λ, contient nécessairement B. Un sous-groupe H qui contient Λ contient tous les produits et les inverses d'éléments de Λ, donc à fortiori tous les éléments de la forme $a_1^{\alpha_1}...\,a_m^{\alpha_m}$ où $m \in \mathbb{N}$, $\alpha_i \in \mathbb{Z}$ et $a_i \in \Lambda$. Donc $B \subset H$.

Remarque : On peut encore écrire $< \Lambda >$ sous la forme

$$< \Lambda > = \left\{a_1^{\alpha_1}...\,a_m^{\alpha_m} \,/\, m \in \mathbb{N},\ \alpha_i \in \{-1, 0, 1\}\,,\ a_i \in \Lambda\right\},$$

la preuve restant la même.

Chapitre 6

CAPES externe 2007, épreuve 2

6.1 Énoncé

INTRODUCTION

Dans tout le problème, n désigne un entier naturel non nul. On munit $\mathbb{R}^n$ du produit scalaire usuel :

$$\forall x = (x_1, ..., x_n) \in \mathbb{R}^n \quad \forall y = (y_1, ..., y_n) \in \mathbb{R}^n \quad \langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

et on définit la norme d'un vecteur $x = (x_1, ..., x_n)$ par

$$||x|| = \sqrt{\sum_{i=1}^{n} x_i^2}.$$

Soit a un vecteur de $\mathbb{R}^n$ non nul, on note s_a la symétrie orthogonale de $\mathbb{R}^n$ dans $\mathbb{R}^n$ définie par

$$\forall x \in \mathbb{R}^n \qquad s_a(x) = x - 2\frac{\langle a, x \rangle}{\langle a, a \rangle} a.$$

On dit qu'une partie R de $\mathbb{R}^n$ est un **système de racines** dans $\mathbb{R}^n$ si elle vérifie les conditions suivantes :

- la partie R est finie, ne contient pas 0 et engendre le $\mathbb{R}$-espace vectoriel $\mathbb{R}^n$;
- pour tout $\alpha \in R$, $s_\alpha(R) = R$ (en particulier $-\alpha \in R$) ;
- pour tous $\alpha, \beta \in R$, $n_{\alpha,\beta} = 2\dfrac{\langle \alpha, \beta \rangle}{\langle \alpha, \alpha \rangle} \in \mathbb{Z}$;

- pour tout $\alpha \in R$, les seuls éléments de R proportionnels à α sont α et $-\alpha$.

Les coefficients $n_{\alpha,\beta}$ sont appelés les **coefficients de structure** du système de racines R.
On dit que deux systèmes de racines R et R' sont des **systèmes de racines isomorphes** s'il existe un isomorphisme d'espaces vectoriels $\varphi : \mathbb{R}^n \to \mathbb{R}^n$ vérifiant

$$\varphi(R) = R' \quad \text{et} \quad \forall \alpha, \beta \in R \qquad n_{\varphi(\alpha),\varphi(\beta)} = n_{\alpha,\beta}.$$

Dans la partie I, on étudie les systèmes de racines du plan. Cette partie permet de se familiariser avec cette notion et d'avoir des exemples sur lesquels s'appuyer pour la suite du problème. Puis dans la partie II, on étudie des relations d'ordre total compatibles avec la structure d'espace vectoriel de $\mathbb{R}^n$. Cette partie est indépendante de la partie I. Ces relations d'ordre permettront, dans la partie III, d'extraire d'un système de racines une base de $\mathbb{R}^n$. Même si le fait d'avoir traité la partie I permet de mieux aborder celle-ci, le seul résultat utile est rappelé en début de la partie III et pourra être admis. Seule la dernière question dépend de la partie I. La partie IV est consacrée à l'étude d'un groupe engendré par les symétries associées à un système de racines. On montrera que les symétries associées à une base suffisent à engendrer le groupe. Pour cela, on utilisera des résultats établis dans la partie III. Ensuite, dans la partie V, on étudiera les groupes diédraux et on montrera qu'ils sont engendrés par deux éléments d'ordre 2. Cette partie est indépendante de ce qui précède (sauf pour traiter la dernière question). Dans la partie VI, on associe à un système de racines un ensemble de parties connexes de $\mathbb{R}^n$ sur lesquels agit le groupe défini dans la partie IV. On montre ensuite, par des arguments de dualité et de topologie, que toutes les bases extraites du système de racines sont en bijection avec ces connexes. Cette partie se finit en montrant que le groupe agit simplement transitivement sur l'ensemble de ces connexes et sur l'ensemble des bases du système de racines.

Partie I. SYSTÈMES DE RACINES DANS $\mathbb{R}^2$

Dans cette partie, on supposera $n = 2$. Soit R un système de racines de $\mathbb{R}^2$. Pour $\alpha, \beta \in R$, on note $\theta_{\alpha,\beta}$ l'angle géométrique entre α et β, i.e. le nombre réel compris entre 0 et π défini par

$$\cos(\theta_{\alpha,\beta}) = \frac{\langle \alpha, \beta \rangle}{||\alpha|| \, ||\beta||}.$$

1. Soit $\alpha, \beta \in R$.
   a) Montrer que $n_{\alpha,\beta}\, n_{\beta,\alpha} = 4\cos^2(\theta_{\alpha,\beta})$.
   b) En déduire les valeurs possibles de $\theta_{\alpha,\beta}$.

c) Montrer que le couple $(n_{\alpha,\beta}, n_{\beta,\alpha})$ ne peut pas prendre les valeurs $(1,4)$, $(4,1)$, $(-1,-4)$ et $(-4,-1)$.

d) Pour $\theta_{\alpha,\beta} \neq \frac{\pi}{2}$, montrer que $\frac{||\alpha||^2}{||\beta||^2} = \frac{n_{\beta,\alpha}}{n_{\alpha,\beta}}$ et déduire les valeurs possibles du rapport $\frac{||\alpha||}{||\beta||}$.

e) En supposant $||\alpha|| \leq ||\beta||$, présenter sous forme d'un tableau, les différentes valeurs de $n_{\alpha,\beta}$, $n_{\beta,\alpha}$, $\theta_{\alpha,\beta}$ et $\frac{||\beta||}{||\alpha||}$.

2. Dessiner les figures correspondant à quatre systèmes de racines dans $\mathbb{R}^2$ non deux à deux isomorphes (dans chacun des cas, l'une des racines devra être $(1,0)$). On les ordonnera dans l'ordre croissant du nombre de racines et on les appellera $A_1 \times A_1$, A_2, B_2 et G_2 (ayant respectivement 4, 6, 8 et 12 racines).

3. Soit α une racine de R de norme minimale. Supposons qu'il existe une racine β de R non proportionnelle et non orthogonale à α. Quitte à transformer R par une rotation, une homothétie ou une symétrie orthogonale d'axe $\mathbb{R} \times \{0\}$ (qui laissent invariants les coefficients de structure du système de racines), on peut supposer $\alpha = (1,0)$ et β de deuxième coordonnée strictement positive.

a) Montrer que $n_{\alpha,\beta} \neq 0$. En posant $\gamma = s_\alpha(\beta)$ montrer que $n_{\alpha,\gamma} = -n_{\alpha,\beta}$.

Quitte à remplacer β par $s_\alpha(\beta)$, on supposera $n_{\alpha,\beta} < 0$ et d'après le tableau des valeurs de $\theta_{\alpha,\beta}$, trois cas peuvent se présenter.

b) **cas 1** : Supposons que $||\beta|| = \sqrt{2}||\alpha||$ et $\theta_{\alpha,\beta} = 3\pi/4$. Calculer $s_\alpha(\beta)$ et $s_\beta(\alpha)$ et représenter graphiquement les quatre racines α, β, $s_\alpha(\beta)$ et $s_\beta(\alpha)$. En déduire que $B_2 \subset R$. En supposant qu'il existe $\gamma \in R\backslash B_2$, montrer qu'alors l'angle entre γ et une racine de B_2 est inférieur à $\pi/8$. En conclure que $R = B_2$.

c) **cas 2** : Supposons que $||\beta|| = \sqrt{3}||\alpha||$ et $\theta_{\alpha,\beta} = 5\pi/6$. Calculer

$$s_\alpha(\beta), \quad s_\beta(\alpha), \quad s_\beta \circ s_\alpha(\beta) \quad \text{et} \quad s_\alpha \circ s_\beta(\alpha)$$

et les représenter graphiquement ainsi que α et β. En déduire que $G_2 \subset R$. En raisonnant par l'absurde, montrer que $R = G_2$.

d) **cas 3** : Supposons que $||\beta|| = ||\alpha||$ et $\theta_{\alpha,\beta} = 2\pi/3$. Calculer $s_\alpha(\beta)$ et en déduire que $A_2 \subset R$. Supposons que $R \neq A_2$, soit $\gamma \in R\backslash A_2$. Montrer que l'angle entre γ et deux vecteurs adjacents de A_2 est égal à $\pi/6$. Quitte à réindexer les éléments de A_2, montrer qu'on peut supposer $\theta_{\alpha,\gamma} = 5\pi/6$. En déduire que $R = A_2$.

4. En conclure qu'à isomorphisme près, il n'y a que quatre systèmes de

racines dans $\mathbb{R}^2$.

Partie II. RELATIONS D'ORDRE DANS $\mathbb{R}^n$

Une relation d'ordre $\preceq$ sur $\mathbb{R}^n$ est dite compatible avec la structure d'espace vectoriel de $\mathbb{R}^n$ si elle vérifie les deux conditions suivantes :

- $\forall x, y, z \in \mathbb{R}^n \qquad x \preceq y \;\Rightarrow\; x + z \preceq y + z$;
- $\forall x, y \in \mathbb{R}^n \qquad \forall \lambda \in \mathbb{R}_+ \qquad x \preceq y \;\Rightarrow\; \lambda x \preceq \lambda y.$

La relation d'ordre strict associée est notée $\prec$.

1. Soit $\preceq$ une relation d'ordre total sur $\mathbb{R}^n$ compatible avec la structure d'espace vectoriel.

a) Montrer que

$$\forall x, y \in \mathbb{R}^n \qquad \forall \lambda \in \mathbb{R}_- \qquad x \preceq y \;\Rightarrow\; \lambda y \preceq \lambda x.$$

b) Soit $\varphi \in \mathrm{GL}(\mathbb{R}^n)$ (le groupe linéaire de $\mathbb{R}^n$). On définit une relation par : pour $x, y \in \mathbb{R}^n$, on a $x \preceq' y$ si $\varphi(x) \preceq \varphi(y)$. Montrer que $\preceq'$ est une relation d'ordre total sur $\mathbb{R}^n$ compatible avec la structure d'espace vectoriel.

2. On définit une relation $\preceq$ sur $\mathbb{R}^n$ par : pour $x = (x_1, ..., x_n) \in \mathbb{R}^n$ et $y = (y_1, ..., y_n) \in \mathbb{R}^n$, on a $x \preceq y$ si

$$x = y \quad \text{ou} \quad [x \neq y \text{ et } x_k < y_k \text{ avec } k = \mathrm{Min}\{i \in \{1, ..., n\} \,/\, x_i \neq y_i\}] \,.$$

a) En munissant le plan $\mathcal{P}$ d'un repère $(O, \overrightarrow{u}, \overrightarrow{v})$, représenter graphiquement la partie

$$\{M\,(x, y) \in \mathcal{P} \,/\, (0,0) \preceq (x, y)\}$$

en la hachurant d'une couleur particulière.

b) Montrer que la relation $\preceq$ est une relation d'ordre total sur $\mathbb{R}^n$ compatible avec la structure d'espace vectoriel. Cet ordre est appelé **l'ordre lexicographique**.

Partie III. BASE D'UN SYSTÈME DE RACINES

On supposera n quelconque. Soit R un système de racines de $\mathbb{R}^n$. Les résultats obtenus en I.1.e restent vrais, même si la dimension n'est plus 2. En particulier, pour deux racines $\alpha, \beta \in R$ distinctes, si $n_{\alpha,\beta} > 0$, l'un des deux coefficients $n_{\alpha,\beta}$ ou $n_{\beta,\alpha}$ est égal à 1.

On appelle **base du système de racines** R une partie B de R telle que

- la famille B est une base de l'espace vectoriel $\mathbb{R}^n$,
- tout élément de R est combinaison linéaire d'éléments de B, à coefficients entiers, soit tous positifs ou nuls, soit tous négatifs ou nuls.

L'objet de cette partie est de mettre en évidence de telles bases.

1. On munit $\mathbb{R}^n$ d'une relation d'ordre total $\preceq$ compatible avec la structure d'espace vectoriel. On note alors R^+ l'ensemble des racines positives et R^- l'ensemble des racines négatives, c'est à dire :

$$R^+ = \{\alpha \in R \,/\, 0 \prec \alpha\} \quad \text{et} \quad R^- = \{\alpha \in R \,/\, \alpha \prec 0\}.$$

On appelle **racine simple** une racine positive qui n'est pas somme de deux racines positives et on note B l'ensemble des racines simples.

a) Montrer que tout élément de R^+ est soit dans B, soit somme de deux racines positives strictement plus petites.

b) Montrer que tout élément de R^+ est combinaison linéaire d'éléments de B à coefficients entiers positifs ou nuls. *(Indication : On pourra ordonner les éléments de R^+ et faire une démonstration par récurrence ou raisonner par l'absurde).*

2. Soit deux racines distinctes $\alpha, \beta \in R$.

a) Montrer que si $n_{\alpha,\beta} > 0$, alors $\alpha - \beta \in R$.

b) Supposons que $\alpha, \beta \in B$. Montrer que $\alpha - \beta \notin R$ et $n_{\alpha,\beta} \leq 0$.

3. Soient α_1, ..., α_r, α_{r+1}, ..., $\alpha_s \in B$ des racines simples deux à deux distinctes et soient λ_1, ..., λ_r, λ_{r+1}, ..., λ_s des réels positifs tels que

$$\lambda_1\alpha_1 + ... + \lambda_r\alpha_r = \lambda_{r+1}\alpha_{r+1} + ... + \lambda_s\alpha_s.$$

Montrer que les réels λ_1, ..., λ_r, λ_{r+1}, ..., λ_s sont tous nuls. *(Indication : On pourra poser $v = \lambda_1\alpha_1 + ... + \lambda_r\alpha_r$ et montrer que $\langle v, v\rangle < 0$.)*

4. Montrer que B est une base de l'espace vectoriel $\mathbb{R}^n$. (On dit que B est une base du système de racines R, associée à l'ordre sur $\mathbb{R}^n$).

5. En munissant $\mathbb{R}^2$ de l'ordre lexicographique, pour chacun des quatre systèmes de racines, dessiner d'une couleur particulière les vecteurs de la base associée.

Partie IV. GROUPE DE WEYL D'UN SYSTÈME DE RACINES

Soit R un système de racines de $\mathbb{R}^n$, $\preceq$ une relation d'ordre total sur $\mathbb{R}^n$ compatible avec la structure d'espace vectoriel, R^+ l'ensemble des racines positives et B la base de R associée à la relation d'ordre. On appelle groupe de Weyl de R, noté W, le sous-groupe des automorphismes de l'espace vectoriel $\mathbb{R}^n$, engendré par les symétries s_α ($\alpha \in R$).

1. Soit $a \in \mathbb{R}^n$ et soit $\varphi \in \mathrm{O}(\mathbb{R}^n)$ (le groupe orthogonal de $\mathbb{R}^n$). Établir que

$$s_{\varphi(a)} = \varphi \circ s_a \circ \varphi^{-1}.$$

2. Montrer que le groupe de Weyl W est un groupe fini.

3. a) Soit $\alpha \in R^+ \backslash B$. Montrer qu'il existe $\beta \in B$ tel que $\langle \beta, \alpha \rangle > 0$ (*Ind : on pourra utiliser III.1.b et développer* $\langle \alpha, \alpha \rangle$). En déduire que $n_{\beta,\alpha} > 0$ et que $\alpha - \beta \in R^+$.

b) Soit $\alpha \in R^+$ et $\beta \in B$ tels que $\alpha \neq \beta$. Montrer que $s_\beta(\alpha) \in R^+$.

4. On note W_B le sous-groupe de W engendré par les applications $(s_\alpha)_{\alpha \in B}$ et on pose

$$S = \{w(\alpha) \,/\, w \in W_B \text{ et } \alpha \in B\}.$$

a) Montrer que $R^+ \subset S$. (*Ind : On pourra raisonner par l'absurde.*)

b) En déduire que $R = S$. (*Ind : On pourra remarquer que* $s_\alpha(\alpha) = -\alpha$ *pour* $\alpha \in B$.)

c) Conclure que $W = W_B$.

Partie V. GROUPES DIÉDRAUX

1. Soit E un plan affine euclidien orienté. Soit $p \in \mathbb{N}$, $p \geq 2$. On appelle groupe diédral d'ordre $2p$, noté D_{2p}, le groupe des isométries laissant invariant un polygone régulier

$$\mathcal{P}_p = \{M_0, M_1, ..., M_{p-1}\}$$

à p sommets, parcourus dans le sens direct. On posera $M_p = M_0$.

a) Montrer que le sous-groupe C_p de D_{2p} constitué des isométries directes, est un groupe cyclique d'ordre p engendré par la rotation ρ de centre O et d'angle $2\pi/p$ où O est le centre du polygone $\mathcal{P}_p$.

b) Préciser une symétrie orthogonale σ laissant le polygone $\mathcal{P}_p$ invariant.

c) Montrer que

$$D_{2p} = \{\rho^i \circ \sigma^j \,/\, i \in \{0, ..., p-1\} \text{ et } j \in \{0, 1\}\}$$

et en déduire que D_{2p} est un groupe d'ordre $2p$.

d) Soit $k \in \{0, ..., p-1\}$. Montrer que $\sigma \circ \rho^k \circ \sigma = \rho^{p-k}$.

2. Soit G un groupe fini engendré par deux éléments distincts s et s' d'ordre 2. On pose $r = ss'$ et on note p l'ordre de r. On note e l'élément neutre de G.

a) Montrer que G est engendré par r et s.

b) Etablir que $sr = r^{-1}s$, puis que $sr^k = r^{p-k}s$ pour tout $k \in \mathbb{N}$. En déduire que

$$G = \{r^i s^j \,/\, i \in \{0, ..., p-1\} \text{ et } j \in \{0, 1\}\}.$$

c) Montrer que pour tout $k \in \mathbb{N}$, $s \neq r^k$ (*on pourra raisonner par l'absurde et montrer que G serait commutatif, puis que $G = \{e, r\}$*). En déduire que G est d'ordre $2p$.

d) Montrer que G est isomorphe à D_{2p}.

e) Déterminer les groupes de Weyl associés aux systèmes de racines de $\mathbb{R}^2$.

Partie VI. CHAMBRES DE WEYL

Soit R un système de racines de $\mathbb{R}^n$ et W le groupe de Weyl associé. Pour tout $\alpha \in R$, ou note P_α l'hyperplan orthogonal à α.

1. Montrer que $\Omega := \mathbb{R}^n \backslash \bigcup_{\alpha \in R} P_\alpha$ est une partie ouverte de $\mathbb{R}^n$.

La partie Ω est réunion finie disjointe de parties non vides ouvertes connexes de $\mathbb{R}^n$, ce sont les **chambres de Weyl** du système de racines R.

2. Soit C une partie connexe non vide de $\mathbb{R}^n$ incluse dans Ω. Montrer qu'il existe une chambre de Weyl de R contenant C.

3. Montrer que le groupe de Weyl W permute les hyperplans P_α ($\alpha \in R$), ainsi que les chambres de Weyl.

4. Soient C_1 et C_2 deux chambres de Weyl de R et soit $x_1 \in C_1$ et $x_2 \in C_2$.

a) Justifier l'existence d'un élément $w \in W$ tel que

$$||x_1 - w(x_2)|| = \operatorname{Inf}\{||x_1 - w'(x_2)|| \,/\, w' \in W\}.$$

b) On pose $I = \{tx_1 + (1-t)w(x_2) \,/\, t \in [0,1]\}$. Montrer que $I \subset C_1$. (*Indication : On pourra supposer qu'il existe $\alpha \in R$ tel que $I \cap P_\alpha \neq \varnothing$ et montrer qu'il existe $t_0 \in]0,1[$ tel que $\langle t_0 x_1 + (1-t_0)w(x_2), \alpha \rangle = 0$ et que $||x_1 - s_\alpha \circ w(x_2)||^2 < ||x_1 - w(x_2)||^2$*).

c) En déduire $w(C_2) = C_1$. On dit que le groupe W **opère transitivement** sur les chambres de Weyl de R.

5. Soit $B = (\beta_1, ..., \beta_n)$ une base de R et soit $(\beta'_1, ..., \beta'_n)$ la base duale de B pour le produit scalaire de $\mathbb{R}^n$, c'est-à-dire, une famille de vecteurs de $\mathbb{R}^n$ vérifiant

$$\forall i, j \in \{1, ..., n\} \qquad \langle\, \beta_i, \beta'_j \,\rangle = \begin{cases} 1 & \text{si } i = j \\ 0 & \text{sinon.} \end{cases}$$

On pose

$$C\,(B) = \{x \in \mathbb{R}^n \,/\, \langle x, \beta_1 \rangle > 0,\ ...,\ \langle x, \beta_n \rangle > 0\}$$
$$= \left\{ \sum_{i=1}^{n} x_i \beta'_i \,/\, x_1, ..., x_n \in \mathbb{R}_+^* \right\},$$

égalité que l'on ne demandera pas de démontrer.

a) Montrer que $C(B) \subset \Omega$ et qu'il existe une chambre de Weyl C telle que $C(B) \subset C$.

b) Soit $i \in \{1, ..., n\}$ fixé. On pose

$$C_i^+ = \{x \in C \mid \langle x, \beta_i \rangle > 0\} \quad \text{et} \quad C_i^- = \{x \in C \mid \langle x, \beta_i \rangle < 0\}.$$

Montrer que C_i^+ et C_i^- sont des parties ouvertes telles que $C_i^+ \cup C_i^- = C$ et $C_i^+ \cap C_i^- = \varnothing$. En déduire que $C = C_i^+$.

c) En déduire que $C(B) = C$. On dit que $C(B)$ est la **chambre de Weyl fondamentale** relativement à B.

6. Pour chacun des quatre systèmes de racines de $\mathbb{R}^2$, hachurer d'une couleur particulière la chambre de Weyl fondamentale relativement à la base associée à l'ordre lexicographique de $\mathbb{R}^2$.

7. a) Montrer que pour toute chambre de Weyl C de R, il existe une base B de R telle que $C = C(B)$.

b) Montrer que l'application qui à une base B de R associe la chambre $C(B)$ est une bijection de l'ensemble des bases de R sur l'ensemble des chambres de R.

8. Soit B une base de R, R^+ l'ensemble des racines positives et R^- l'ensemble des racines négatives.

a) Soient β_1, ..., β_p ($p \in \mathbb{N}^*$) des éléments non nécessairement distincts de B tels que

$$s_{\beta_1} \circ ... \circ s_{\beta_{p-1}}(\beta_p) \in R^-.$$

Montrer qu'il existe $q \in \{1, ..., p-1\}$ tel que

$$s_{\beta_1} \circ ... \circ s_{\beta_p} = s_{\beta_1} \circ ... \circ s_{\beta_{q-1}} \circ s_{\beta_{q+1}} \circ ... \circ s_{\beta_{p-1}}.$$

b) En déduire que si $w \in W$ et $w \neq Id$, alors il existe $\beta \in B$ tel que $w(\beta) \in R^-$.

9. a) Montrer que le groupe de Weyl W de R **opère simplement transitivement** sur l'ensemble des bases de R, c'est-à-dire que pour deux bases B et B' données de R, il existe un unique élément $w \in W$ tel que $w(B) = B'$.

b) En déduire que le groupe de Weyl W de R opère simplement transitivement sur l'ensemble des chambres de Weyl de R.

6.2 Corrigé

Remarque préliminaire : s_a est la réflexion par rapport à l'hyperplan $(\mathbb{R}a)^{\perp}$ orthogonal à a. En effet, s_a est linéaire, vérifie

$$s_a(a) = a - 2\frac{\langle a, a\rangle}{||a||^2}a = -a$$

et pour tout vecteur x orthogonal à a,

$$s_a(x) = x - 2\frac{\langle a, x\rangle}{||a||^2}a = x.$$

[Entre nous : La preuve donnée ci-dessus est complète, rien n'a été oublié, et il faut pouvoir la dire à l'oral du concours. Ce type de preuve fait partie des "fondamentaux" à connaître et à savoir expliquer. Mieux, cette expression de s_a, utilisée pour ramener le calcul de l'image $s_a(x)$ à celui d'un produit scalaire, est à la base de la méthode de Househölder qui fait partie du programme de l'écrit du CAPES ([15], Chap. 7.6 et Lemme 9).
Cette expression de s_a apparaît régulièrement dans les problèmes de concours, et le candidat possède ici un bon atout s'il l'a connaît.]

Partie I. SYSTEMES DE RACINES DANS $\mathbb{R}^2$

I.1.a. On a

$$n_{\alpha,\beta}\,n_{\beta,\alpha} \;=\; 2\frac{\langle\alpha,\beta\rangle}{||\alpha||^2}\times 2\frac{\langle\beta,\alpha\rangle}{||\beta||^2} \;=\; 4\frac{\langle\alpha,\beta\rangle^2}{||\alpha||^2||\beta||^2} \;=\; 4\cos^2\theta_{\alpha,\beta}.$$

I.1.b. $n_{\alpha,\beta}\,n_{\beta,\alpha} = 4\cos^2\theta_{\alpha,\beta}$ est un entier compris entre 0 et 4, donc

$$\cos\theta_{\alpha,\beta} \in \{0, \pm\frac{1}{2}, \pm\frac{\sqrt{2}}{2}, \pm\frac{\sqrt{3}}{2}, \pm 1\}.$$

Comme $\theta_{\alpha,\beta} \in [0,\pi]$, on aura $\theta_{\alpha,\beta} \in \{\frac{\pi}{2}, \frac{\pi}{3}, \frac{2\pi}{3}, \frac{\pi}{4}, \frac{3\pi}{4}, \frac{\pi}{6}, \frac{5\pi}{6}, 0, \pi\}$.

I.1.c. Si $(n_{\alpha,\beta}, n_{\beta,\alpha})$ prend l'une des valeurs annoncées, $n_{\alpha,\beta}n_{\beta,\alpha} = 4$ donc $\cos^2\theta_{\alpha,\beta} = 1$. Dans ce cas $\theta_{\alpha,\beta} \in \{0,\pi\}$ et les vecteurs α et β sont colinéaires. Comme R est un système de racines, on en déduit $\beta = \pm\alpha$. On ne peut pas avoir $\beta = \alpha$ (autrement $n_{\alpha,\beta} = 0$ ne peut pas vérifier $n_{\alpha,\beta}n_{\beta,\alpha} = 4$), donc $\beta = -\alpha$ et :

$$n_{\alpha,\beta} = 2\frac{\langle\alpha,\beta\rangle}{||\alpha||^2} = -2,$$

ce qui contredit notre choix de $n_{\alpha,\beta}$.

Remarque : On a affirmé que $\theta_{\alpha,\beta} = 0$ ou π si et seulement si les vecteurs α et β sont colinéaires. Il s'agit d'une conséquence directe du cas d'égalité dans l'inégalité de Cauchy-Schwarz puisque :

$$\theta_{\alpha,\beta} = 0 \text{ ou } \pi \quad \Leftrightarrow \quad |\langle \alpha, \beta \rangle| = ||\alpha||\,||\beta|| \quad \Leftrightarrow \quad \alpha \text{ et } \beta \text{ colinéaires.}$$

Ce cas d'égalité fait partie du bagage standard de cours à la disposition du candidat. La preuve de ce résultat de cours doit être connue pour l'écrit comme pour l'oral du concours ([15], Théorème 86).

I.1.d.

$$\frac{n_{\beta,\alpha}}{n_{\alpha,\beta}} = 2\frac{\langle \beta, \alpha \rangle}{||\beta||^2} \times \frac{||\alpha||^2}{2\langle \alpha, \beta \rangle} = \frac{||\alpha||^2}{||\beta||^2}.$$

On envisage tous les cas suivant les valeurs de $\theta_{\alpha,\beta}$ obtenues en I.1.b.

- Si $\theta_{\alpha,\beta} = \frac{\pi}{3}$ ou $\frac{2\pi}{3}$, $n_{\alpha,\beta}\, n_{\beta,\alpha} = 4\cos^2\theta_{\alpha,\beta} = 1$ donc $\frac{||\alpha||^2}{||\beta||^2} = \frac{n_{\beta,\alpha}}{n_{\alpha,\beta}} = 1$.
- Si $\theta_{\alpha,\beta} = \frac{\pi}{4}$ ou $\frac{3\pi}{4}$, $n_{\alpha,\beta}\, n_{\beta,\alpha} = 2$ donc $\frac{||\alpha||^2}{||\beta||^2} = \frac{n_{\beta,\alpha}}{n_{\alpha,\beta}} = \frac{2}{n^2_{\alpha,\beta}}$.
  - Si $n_{\alpha,\beta} = \pm 1$, $\frac{||\alpha||}{||\beta||} = \sqrt{2}$,
  - Si $n_{\alpha,\beta} = \pm 2$, $\frac{||\alpha||}{||\beta||} = \frac{1}{\sqrt{2}}$.
- Si $\theta_{\alpha,\beta} = \frac{\pi}{6}$ ou $\frac{5\pi}{6}$, $n_{\alpha,\beta}\, n_{\beta,\alpha} = 3$ donc $\frac{||\alpha||^2}{||\beta||^2} = \frac{n_{\beta,\alpha}}{n_{\alpha,\beta}} = \frac{3}{n^2_{\alpha,\beta}}$.
  - Si $n_{\alpha,\beta} = \pm 1$, $\frac{||\alpha||}{||\beta||} = \sqrt{3}$,
  - Si $n_{\alpha,\beta} = \pm 3$, $\frac{||\alpha||}{||\beta||} = \frac{1}{\sqrt{3}}$,
- Si $\theta_{\alpha,\beta} = 0$ ou π, $n_{\alpha,\beta}\, n_{\beta,\alpha} = 4$ donc $\frac{||\alpha||^2}{||\beta||^2} = \frac{n_{\beta,\alpha}}{n_{\alpha,\beta}} = \frac{4}{n^2_{\alpha,\beta}}$.

Mais on ne peut avoir ni $n_{\alpha,\beta} = \pm 1$, ni $n_{\alpha,\beta} = \pm 4$ d'après la question I.1.c. Donc $n_{\alpha,\beta} = \pm 2 = n_{\beta,\alpha}$ et $\frac{||\alpha||}{||\beta||} = 1$.

En conclusion : $\frac{||\alpha||}{||\beta||} \in \{1, \sqrt{2}, \frac{1}{\sqrt{2}}, \sqrt{3}, \frac{1}{\sqrt{3}}\}$.

Remarques : Dans le dernier cas où $\theta_{\alpha,\beta} = 0$ ou π, on peut conclure en notant que les vecteurs α et β sont alors colinéaires (comme au I.1.c). Comme α et β appartiennent à un système de racines R, on en déduit $\beta = \pm\alpha$ et $||\alpha||/||\beta|| = 1$.

Remarque stratégique : Au niveau stratégique, cette première partie peut coûter cher en temps. S'il faut bien la commencer et continuer à y travailler tant qu'on a quelque chose à dire, il ne faut pas y rester trop longtemps pour profiter des autres parties du problème. On conservera résolument un oeil sur sa montre !

On peut aussi décider très tôt de sauter la première partie si l'on ne s'y sent pas à l'aise, et récupérer en priorité le maximum de points offerts dans les autres parties, quitte à revenir sur la première partie s'il ne reste plus rien à gagner ailleurs !.

On peut par exemple traiter la Partie II au brouillon en environ 20 min, et la Partie V sur les groupes des polygones réguliers en un peu plus d'une heure (excepté la dernière question qui dépend d'une autre partie), *à partir du moment où l'on a bien révisé ses "fondamentaux"*. La Partie V est "à portée" si l'on a travaillé et *APPROFONDI* la leçon d'oral sur les isométries laissant invariant un polygone régulier ([18], Chap. 9).

Mazette, il serait affligeant de sortir de l'épreuve en n'ayant pas répondu aux questions où nous avions des choses à dire et à montrer, et en s'étant seulement cantonné à la première partie. Gagnons des points en combattant sur notre terrain, montrons ce que nous savons faire et ne peinons pas plus de 2 heures sur une partie qui ne nous mettrait pas en valeur.

Enfin, préparons l'oral du concours même si l'on n'est pas admissible, car une leçon comme celle sur les isométries du polygone régulier nous entraîne merveilleusement pour l'écrit : preuve à la partie V.

I.1.e. Je propose un tableau plus général pour des valeurs quelconques du rapport $||\beta||/||\alpha||$:

$n_{\alpha,\beta}$	$n_{\beta,\alpha}$	$\theta_{\alpha,\beta}$	$\|\|\beta\|\|/\|\|\alpha\|\| = \sqrt{n_{\alpha,\beta}/n_{\beta,\alpha}}$
0	0	$\frac{\pi}{2}$	non défini
±1	±1	$\frac{\pi}{3}$ ou $\frac{2\pi}{3}$	1
±1 ±2	±2 ±1	$\frac{\pi}{4}$ ou $\frac{3\pi}{4}$	$1/\sqrt{2}$ $\sqrt{2}$
±1 ±3	±3 ±1	$\frac{\pi}{6}$ ou $\frac{5\pi}{6}$	$1/\sqrt{3}$ $\sqrt{3}$
±2	±2	0 ou π	1 (ici : $\beta = \pm\alpha$)

I.2. La FIG. 6.1 montre quatre systèmes de racines de $\mathbb{R}^2$ non deux à deux

isomorphes.

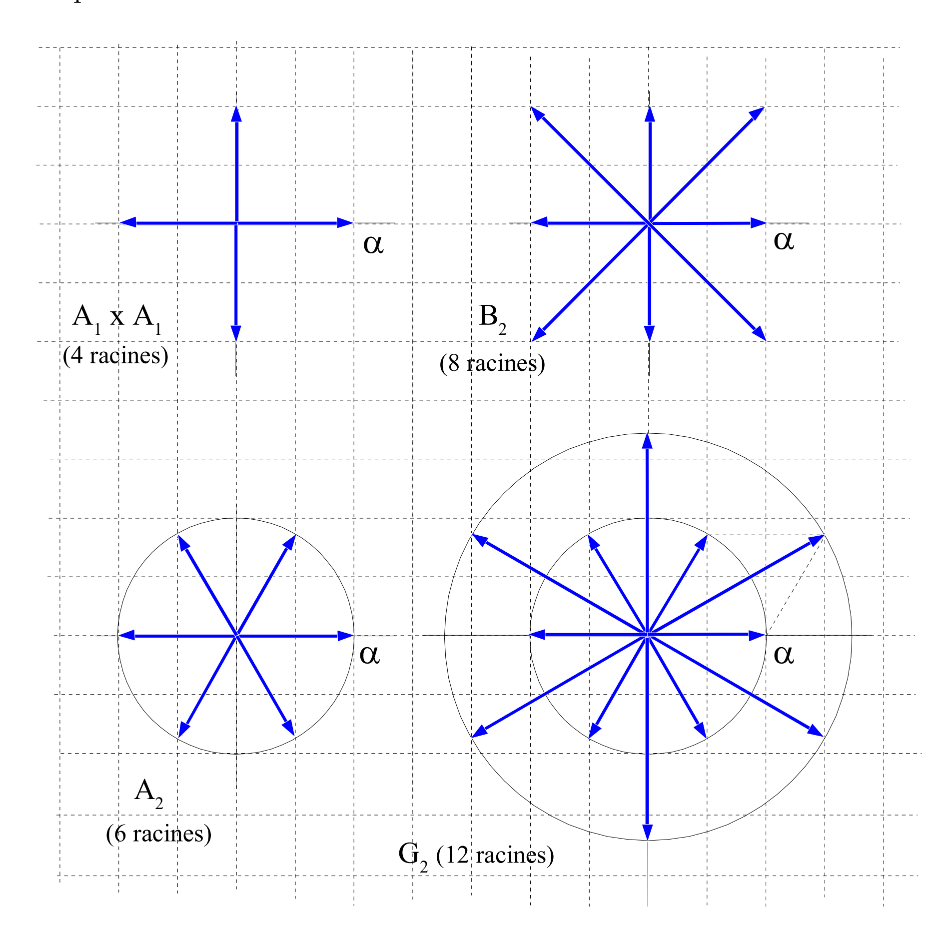


FIG. 6.1 – Quatre systèmes de racines dans $\mathbb{R}^2$

Remarques : α) Le tableau de la question I.1.e nous permet d'obtenir les quatre systèmes de la FIG. 6.1. On commence par tracer $\alpha = (1,0)$, puis on dessine au brouillon des vecteurs β faisant des angles de $\pi/2$, $\pi/4$, $\pi/3$, $\pi/6$ avec α.

β) Dans mon premier essai "au brouillon" sur la partie I, j'ai traité toutes les questions I.1 à I.3.b incluse en 1h40. Cela a pris beaucoup de temps, et si toutes les questions traitées l'ont été à un niveau de satisfaction convenable, cela n'a pas été le cas pour cette question I.2 : je pensais d'abord proposer quatre polygones réguliers, puis j'ai seulement réussi à donner les deux premiers dessins $A_1 \times A_1$ et B_2 après y être retourné au moment de traiter la question III.5.

γ) Voyons comment obtenir l'un des dessins de la FIG. 6.1. Prenons par exemple la cas où $\theta_{\alpha,\beta} = \pi/4$. Dans cette situation, $\alpha = (1,0)$ et $\beta = t\,(1,1)$ avec $t \in \mathbb{R}$ et

$$n_{\alpha,\beta} = 2\frac{\langle \alpha, \beta \rangle}{||\alpha||^2} = 2t,$$

où $n_{\alpha,\beta} = 1$ ou 2 (d'après le tableau de la question I.1.e).

- Si $n_{\alpha,\beta} = 1$, $t = 1/2$ et $\beta = (1/2, 1/2)$.
- Si $n_{\alpha,\beta} = 2$, $t = 1$ et $\beta = (1,1)$.

On obtient donc deux configurations possibles (a) et (b) représentés sur la FIG. 6.2. Ces deux systèmes de racines sont clairement isomorphes puisqu'on peut passer de l'un à l'autre par une similitude directe (une composée d'une rotation et d'une homothétie de centres l'origine du repère). Il est donc naturel de ne retenir qu'une seule configuration dans la FIG. 6.1 : j'ai retenu la configuration (b).
Le travail est identique pour les autres valeurs de $\theta_{\alpha,\beta}$ et l'on n'obtient finalement 4 configurations.

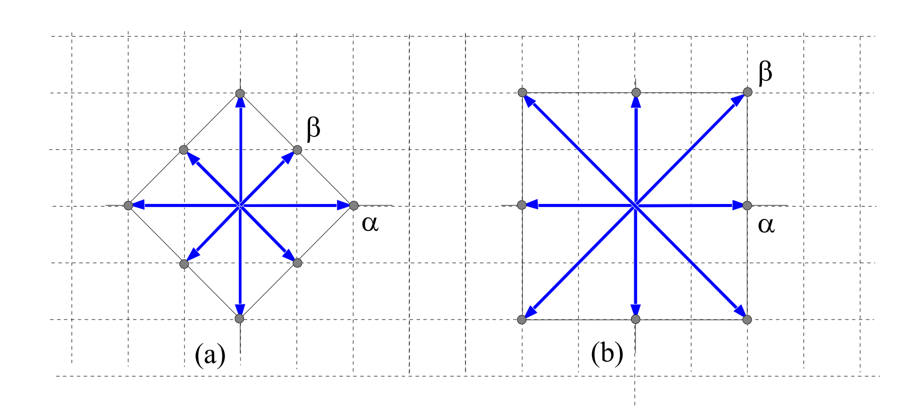


FIG. 6.2 – Cas où $\theta_{\alpha,\beta} = \pi/4$.

I.3.a. • On a

$$n_{\alpha,\beta} = 0 \quad \Leftrightarrow \quad \langle \alpha, \beta \rangle = 0 \quad \Leftrightarrow \quad \alpha \text{ et } \beta \text{ orthogonaux.}$$

Comme α et β ne sont ni colinéaires, ni orthogonaux, on en déduit $n_{\alpha,\beta} \neq 0$.

• Par ailleurs $\gamma = s_\alpha(\beta) = \beta - n_{\alpha,\beta}\alpha$, donc

$$\begin{aligned} n_{\alpha,\gamma} = 2\frac{\langle \alpha, \gamma\rangle}{||\alpha||^2} &= \frac{2}{||\alpha||^2}\langle \alpha, \beta - n_{\alpha,\beta}\alpha\rangle \\ &= 2\frac{\langle \alpha, \beta\rangle}{||\alpha||^2} - n_{\alpha,\beta}\frac{2\langle \alpha, \alpha\rangle}{||\alpha||^2} = n_{\alpha,\beta} - 2n_{\alpha,\beta} = -n_{\alpha,\beta}. \end{aligned}$$

I.3.b. • Ici $\langle \alpha, \beta\rangle = ||\alpha||\,||\beta||\cos\theta_{\alpha,\beta} = \sqrt{2}||\alpha||^2 \times (-\frac{1}{\sqrt{2}}) = -1$, donc

$$\begin{cases} s_\alpha(\beta) = \beta - 2\frac{\langle \alpha, \beta\rangle}{||\alpha||^2}\alpha = \beta + 2\alpha \\ s_\beta(\alpha) = \alpha - 2\frac{\langle \beta, \alpha\rangle}{||\beta||^2}\beta = \alpha + \beta. \end{cases}$$

D'après la remarque prémilinaire, $s_\alpha(\beta)$ est le symétrique de β par rapport à la droite $(\mathbb{R}\alpha)^\perp$ orthogonale à α. Il est donc facile de tracer $s_\alpha(\beta)$ (et $s_\beta(\alpha)$) sur la FIG. 6.3. Les vecteurs α et β appartenant à R, on peut affirmer que $s_\alpha(\beta)$ et $s_\beta(\alpha)$ aussi.

• Si $x \in R$, alors $-x \in R$. Les symétriques des quatre vecteurs α, β, $s_\alpha(\beta)$ et $s_\beta(\alpha)$ appartiennent donc aussi à R, et les 8 vecteurs de B_2 seront dans R. Ainsi $B_2 \subset R$.

• Un vecteur γ appartenant à $R \backslash B_2$ sera forcément dessiné dans l'un des secteurs angulaires délimités par deux demi-droites faisant un angle polaire de $k2\pi/8$ et $(k+1)2\pi/8$ $(k \in \mathbb{Z})$, et l'angle géométrique entre γ et au moins un vecteur de B_2 sera $\leq \pi/8$. C'est absurde d'après le tableau I.1.e. Ainsi $R \subset B_2$, et l'on peut conclure à $R = B_2$.

I.3.c. Ici $\langle \alpha, \beta\rangle = ||\alpha||\,||\beta||\cos\theta_{\alpha,\beta} = \sqrt{3}||\alpha||^2 \times (-\frac{\sqrt{3}}{2}) = -\frac{3}{2}$, donc

$$\begin{cases} s_\alpha(\beta) = \beta - 2\frac{\langle \alpha, \beta\rangle}{||\alpha||^2}\alpha = 3\alpha + \beta \\ s_\beta(\alpha) = \alpha - 2\frac{\langle \beta, \alpha\rangle}{||\beta||^2}\beta = \alpha + \beta. \end{cases}$$

$$s_\beta \circ s_\alpha(\beta) = s_\beta(3\alpha + \beta) = 3s_\beta(\alpha) + s_\beta(\beta) = 3(\alpha + \beta) - \beta = 3\alpha + 2\beta$$

$$s_\alpha \circ s_\beta(\alpha) = s_\alpha(\alpha + \beta) = s_\alpha(\alpha) + s_\alpha(\beta) = -\alpha + (3\alpha + \beta) = 2\alpha + \beta$$

Ces vecteurs sont représentés sur la FIG. 6.4. Les opposés de ces vecteurs appartiennent aussi à R et ont été aussi dessinés sur le figure. On en déduit l'inclusion $G_2 \subset R$.

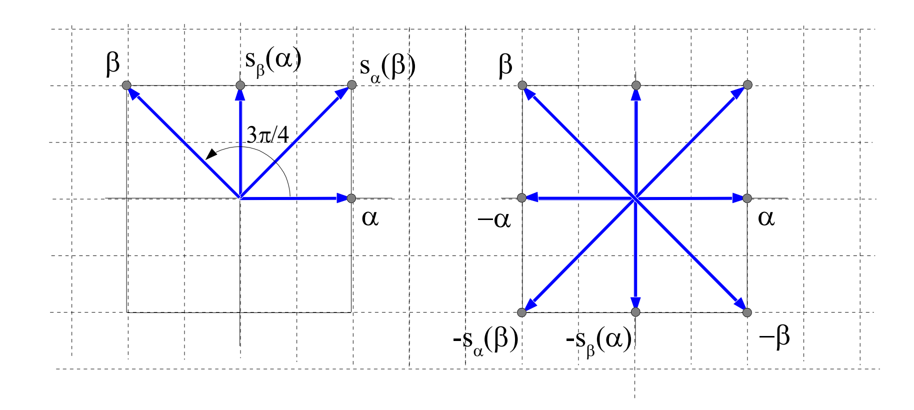


FIG. 6.3 – Question I.3.b

S'il existait un vecteur γ dans $R \backslash G_2$, l'angle qu'il ferait avec au moins un des vecteurs de G_2 serait $\leq \pi/12$, ce qui est impossible d'après le tableau I.1.e.

I.3.d. Ici $\langle \alpha, \beta \rangle = ||\alpha|| \, ||\beta|| \, \cos \theta_{\alpha,\beta} = ||\alpha||^2 \times (-\frac{1}{2}) = -\frac{1}{2}$, donc

$$s_\alpha (\beta) = \beta - 2\frac{\langle \alpha, \beta \rangle}{||\alpha||^2}\alpha = \alpha + \beta.$$

Les vecteurs α, β, $\alpha + \beta$ et leurs opposés appartiennent ainsi à R, et l'on en déduit $A_2 \subset R$.
Un vecteur γ de $R \backslash A_2$ appartient à au moins un secteur angulaire délimité par deux demi-droites d'origine $(0, 0)$ dirigées par deux vecteurs adjacents de A_2. Un tel secteur mesure moins de $\pi/3$ radians, donc l'angle entre γ et au moins un vecteur de A_2 est $\leq \pi/6$. Cet angle ne pouvant pas être strictement inférieur à $\pi/6$ d'après le tableau I.1.e, il sera égal à $\pi/6$.
En réindexant éventuellement les éléments de A_2 (donc en choisissant au besoin un autre élément de A_2 que l'on notera α), on peut supposer que

$$\theta_{\alpha,\gamma} = \frac{\pi}{3} + \frac{\pi}{3} + \frac{\pi}{6} = \frac{5\pi}{6}.$$

C'est impossible compte tenu du tableau I.1.e.
Finalement $R \backslash A_2 = \varnothing$, donc $R \subset A_2$. L'inclusion inverse ayant déjà été montrée, on conclut à $R = A_2$.

I.4. Tous les cas ont été envisagés en I.3, et l'on a donc montré qu'un système de racines de $\mathbb{R}^2$ ne pouvait être (à isomorphisme près) que l'un des quatre systèmes exhibés à la question I.2. Ceux-ci conviennent.

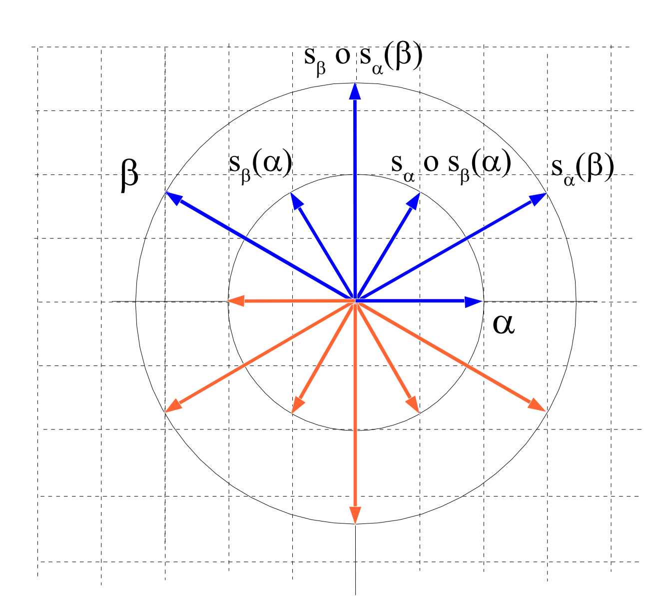


FIG. 6.4 – Question I.3.c

Partie II. RELATIONS D'ORDRE DANS $\mathbb{R}^n$

II.1.a. Si $\lambda \in \mathbb{R}_-$, $-\lambda$ est positif et :

$$\begin{aligned} x \preceq y &\Rightarrow (-\lambda)\, x \preceq (-\lambda)\, y \\ &\Rightarrow -\lambda x + (\lambda x + \lambda y) \preceq -\lambda y + (\lambda x + \lambda y) \\ &\Rightarrow \lambda y \preceq \lambda x \end{aligned}$$

pour tout $x, y \in \mathbb{R}^n$.

II.1.b. • $\preceq'$ est <u>réflexive</u> puisque $x \preceq x$ pour tout $x \in \mathbb{R}^n$. En effet, $x \preceq x$ équivaut à $\varphi(x) \preceq \varphi(x)$, et cette dernière inégalité est triviale.

• $\preceq'$ est <u>antisymétrique</u> puisque

$$\left\{ \begin{array}{l} x \preceq' y \\ y \preceq' x \end{array} \right. \Leftrightarrow \left\{ \begin{array}{l} \varphi(x) \preceq \varphi(y) \\ \varphi(y) \preceq \varphi(x) \end{array} \right. \Rightarrow \varphi(x) = \varphi(y) \Rightarrow x = y,$$

la dernière implication provenant du fait que φ est un automorphisme de $\mathbb{R}^n$ (c'est donc une application injective).

• $\preceq'$ est transitive puisque

$$\left\{\begin{array}{l} x \preceq' y \\ y \preceq' z \end{array}\right. \Leftrightarrow \left\{\begin{array}{l} \varphi(x) \preceq \varphi(y) \\ \varphi(y) \preceq \varphi(z) \end{array}\right. \Rightarrow \varphi(x) \preceq \varphi(y) \preceq \varphi(z)$$
$$\Rightarrow \varphi(x) \preceq \varphi(z)$$
$$\Rightarrow x \preceq' z.$$

• Les trois points précédents montrent que $\preceq'$ est une relation d'ordre. C'est une relation d'ordre total car deux éléments x, y de $\mathbb{R}^n$ sont toujours comparables. En effet, si x, y sont donnés, on a $\varphi(x) \preceq \varphi(y)$ ou $\varphi(y) \preceq \varphi(x)$, donc $x \preceq' y$ ou $y \preceq' x$.

• Il ne reste plus qu'à vérifier que $\preceq'$ est compatible avec la structure d'espace vectoriel. On vérifie les deux assertions de la définition de cette compatibilité. Pour tous $x, y, z \in \mathbb{R}^n$, en utilisant la linéarité de φ :

$$x \preceq' y \Leftrightarrow \varphi(x) \preceq \varphi(y) \Rightarrow \varphi(x) + \varphi(z) \preceq \varphi(y) + \varphi(z)$$
$$\Rightarrow \varphi(x+z) \preceq \varphi(y+z)$$
$$\Rightarrow x + z \preceq' y + z.$$

Si $\lambda \in \mathbb{R}_+$ et $x, y \in \mathbb{R}^n$,

$$x \preceq' y \Leftrightarrow \varphi(x) \preceq \varphi(y) \Rightarrow \lambda\varphi(x) \preceq \lambda\varphi(y)$$
$$\Rightarrow \varphi(\lambda x) \preceq \varphi(\lambda y)$$
$$\Rightarrow \lambda x \preceq' \lambda y.$$

II.2.a. On a

$$(0,0) \preceq (x,y) \Leftrightarrow \left\{\begin{array}{l} x = 0 \text{ et } y = 0 \\ \text{ou} \\ x = 0 \text{ et } 0 < y \\ \text{ou} \\ 0 < x. \end{array}\right.$$

Dans la FIG. 6.5, on a hachuré l'ensemble des (x,y) tels que $(0,0) \preceq (x,y)$. Cet ensemble est la réunion du demi-plan ouvert $x > 0$ et de la demi-droite ouverte $\{x = 0,\ y \geq 0\}$ incluse dans la frontière de ce demi-plan.

II.2.b. • Par définition, $x = x$ entraîne $x \preceq x$. La relation $\preceq$ est donc réflexive.

• $\preceq$ est-elle antisymétrique ? Soient x et y tels que $x \preceq y$ et $y \preceq x$. Si $x = y$, tout est parfait. Sinon, posons $k = \mathrm{Min}\{i \in \{1, ..., n\} \,/\, x_i \neq y_i\}$. Par définition de $\preceq$, on a $x_k < y_k$ et $y_k < x_k$, d'où $x_k = y_k$, ce qui est absurde. Donc

$$\left\{\begin{array}{l} x \preceq y \\ y \preceq x \end{array}\right. \Rightarrow \quad x = y,$$

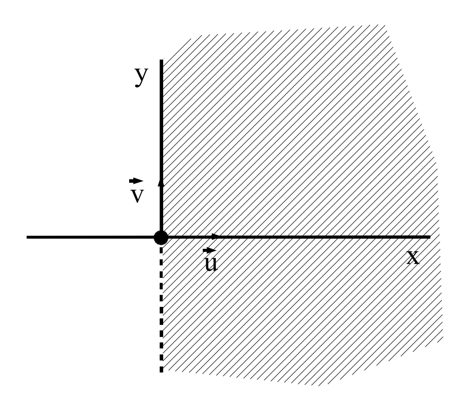


FIG. 6.5 – $\{M\,(x,y) \in \mathcal{P}\,/\,\,(0,0) \preceq (x,y)\}$ est hachuré

et $\preceq$ est bien antisymétrique.

• $\preceq$ est-elle transitive ? Si $x \preceq y$ et $y \preceq z$, deux cas se présentent :

α) Si $x = y$ ou $y = z$, on obtient évidemment $x \preceq z$.

β) Si $x \neq y$ et $y \neq z$, on définit $k = \text{Min}\{i \in \{1, ..., n\}\,/\,x_i \neq y_i\}$ et $l = \text{Min}\{i \in \{1, ..., n\}\,/y_i \neq z_i\}$. Les hypothèses se traduisent par $x_k < y_k$ et $y_l < z_l$; et trois cas sont à envisager :

- Si $k < l$, $x_k < y_k = z_k$ et $x_i = y_i = z_i$ pour tout $i < k$, donc $x \preceq z$.
- Si $k = l$, $x_k < y_k < z_k$ et $x_i = y_i = z_i$ pour tout $i < k$, donc $x \preceq z$.
- Si $k > l$, $x_l = y_l < z_l$ et $x_i = y_i = z_i$ pour tout $i < l$, donc $x \preceq z$.

En conclusion
$$\begin{cases} x \preceq y \\ y \preceq z \end{cases} \Rightarrow \quad x \preceq z,$$
et $\preceq$ est transitive.

• On vient de prouver que $\preceq$ était une relation d'ordre. Considérons deux vecteurs x et y distincts. Il existe alors un indice i tel que $x_i \neq y_i$, et la partie $\{i \in \{1, ..., n\}\,/\,x_i \neq y_i\}$ est incluse dans $\mathbb{N}$ et n'est pas vide, donc admet un minimum $k = \text{Min}\{i \in \{1, ..., n\}\,/\,x_i \neq y_i\}$. Deux possibilités s'offrent alors à nous :

- Ou bien $x_k < y_k$, et alors $x \preceq y$;
- Ou bien $y_k < x_k$, et dans ce cas $y \preceq x$.

Ainsi
$$\forall x, y \in \mathbb{R}^n \quad x \preceq y \text{ ou } y \preceq x,$$
et $\preceq$ est une relation d'ordre total.

• Montrons que $\preceq$ est compatible avec la structure d'espace vectoriel. L'implication

$$\forall x, y, z \in \mathbb{R}^n \qquad x \preceq y \ \Rightarrow \ x + z \preceq y + z$$

est évidente si $x = y$. Si $x \neq y$, et en supposant par exemple $x \prec y$, on a $x_k < y_k$ où $k = \operatorname{Min}\{i \in \{1, ..., n\} \,/\, x_i \neq y_i\}$. Par suite $x_k + z_k < y_k + z_k$ où $k = \operatorname{Min}\{i \in \{1, ..., n\} \,/\, x_i + z_i \neq y_i + z_i\}$, et cela signifie que $x + z \preceq y + z$.
Enfin l'implication

$$\forall x, y \in \mathbb{R}^n \qquad \forall \lambda \in \mathbb{R}_+ \qquad x \preceq y \ \Rightarrow \ \lambda x \preceq \lambda y$$

est triviale si $x = y$ ou si $\lambda = 0$, et se démontre facilement si $x \neq y$ et $\lambda \neq 0$. Dans ce dernier cas, en effet, si l'on suppose $x \prec y$, on peut écrire $x_k < y_k$ avec $k = \operatorname{Min}\{i \in \{1, ..., n\} \,/\, x_i \neq y_i\}$, et l'on obtient $\lambda x_k < \lambda y_k$ avec $k = \operatorname{Min}\{i \in \{1, ..., n\} \,/\, \lambda x_i \neq \lambda y_i\}$, c'est-à-dire $\lambda x \preceq \lambda y$ comme désiré.

Partie III. BASE D'UN SYSTEME DE RACINES

III.1.a. Si $\alpha \in R^+$, de deux choses l'une :

• Ou bien $\alpha \in B$,

• Ou bien $\alpha \notin B$, et α est somme de deux racines positives. Si l'on note $\alpha = \beta + \gamma$, avec $\beta, \gamma \in R^+$, on peut écrire

$$\beta \in R^+ \ \Rightarrow \ 0 \prec \beta \ \Rightarrow \ \gamma \prec \beta + \gamma \ \Rightarrow \ \gamma \prec \alpha$$

et

$$\gamma \in R^+ \ \Rightarrow \ 0 \prec \gamma \ \Rightarrow \ \beta \prec \beta + \gamma \ \Rightarrow \ \beta \prec \alpha.$$

Dans ce cas, α est somme de deux racines positives strictement plus petites.

III.1.b. Comme R est fini, on peut énumérer les éléments de R^+ dans l'ordre croissant et écrire $R^+ = \{\xi_1, \xi_2, ..., \xi_m\}$ avec $\xi_1 \prec \xi_2 \prec ... \prec \xi_m$.
On montre alors la propriété suivante par récurrence finie sur k :

> $H(k)$: "Chacun des éléments ξ_1, ξ_2, ..., ξ_k est combinaison linéaire d'éléments de B à coefficients dans $\mathbb{N}$."

• La propriété $H(1)$ est triviale puisque ξ_1 appartient à B. Dans le cas contraire, III.1.a montrerait l'existence de $\beta, \gamma \in R^+$ tels que $\xi_1 = \beta + \gamma$, $\beta \prec \xi_1$ et $\gamma \prec \xi_1$, ce qui est impossible puisqu'il n'existe pas de racine de R^+ strictement inférieure à ξ_1.

• Si $H(k)$ est vraie (avec $1 \leq k < m$) montrons que $H(k+1)$ est vraie. Pour cela, il suffit de démontrer que ξ_{k+1} est combinaison linéaire d'éléments de B à coefficients dans $\mathbb{N}$. De deux choses l'une :

• Ou bien $\xi_{k+1} \in B$, et c'est fini !

• Ou bien $\xi_{k+1} \notin B$, et il existe $\beta, \gamma \in R^+$ tels que $\xi_{k+1} = \beta + \gamma$, $\beta \prec \xi_{k+1}$ et $\gamma \prec \xi_{k+1}$ (III.1.a). Il existe alors i et j appartenant à $\{1, ..., k\}$ tels que

$\beta = \xi_i$ et $\gamma = \xi_j$. L'hypothèse récurrente au rang k montre que β et γ sont des combinaisons linéaires d'éléments de B à coefficients dans $\mathbb{N}$, et il en sera de même de $\xi_{k+1} = \beta + \gamma$.

Autre solution : Notons Λ la partie de R^+ formée des racines qui ne s'écrivent pas comme combinaisons linéaires d'éléments de B à coefficients dans $\mathbb{N}$, et supposons par l'absurde que $\Lambda \neq \varnothing$. Comme R^+ est un ensemble fini totalement ordonné par $\preceq$, Λ possède un minimum. Posons $\mu = \operatorname{Min} \Lambda$. D'après III.1.a, deux cas sont seulement possibles :

- Ou bien $\mu \in B$, mais cela ne peut pas être puisque $\mu \in \Lambda$.
- Ou bien $\mu = \beta + \gamma$ avec $\beta, \gamma \in R^+$, $\beta \prec \mu$ et $\gamma \prec \mu$. C'est ennuyeux car β et γ étant strictement inférieurs à μ, ils seront combinaisons linéaires d'éléments de B à coefficients dans $\mathbb{N}$, et leur somme $\mu = \beta + \gamma$ aussi, ce qui est impossible.

Dans tous les cas, on obtient une absurdité, et l'on peut conclure à $\Lambda = \varnothing$.

III.2.a. Si $n_{\alpha,\beta} > 0$, alors $n_{\alpha,\beta} = 1$ ou $n_{\beta,\alpha} = 1$. Si par exemple $n_{\alpha,\beta} = 1$, alors $s_\alpha(\beta) = \beta - n_{\alpha,\beta}\alpha = \beta - \alpha$ et les propriétés de R nous permettent d'écrire

$$\alpha, \beta \in R \quad \Rightarrow \quad s_\alpha(\beta) \in R \quad \Rightarrow \quad -s_\alpha(\beta) = \alpha - \beta \in R.$$

Le cas où $n_{\beta,\alpha} = 1$ se traite de la même façon.

III.2.b. Montrons les implications

$$\alpha, \beta \in B \overset{(1)}{\Rightarrow} \alpha - \beta \notin R \overset{(2)}{\Rightarrow} n_{\alpha,\beta} \leq 0.$$

L'implication (2) est la contraposée de l'implication du III.2.a. Montrons (1) en raisonnant par l'absurde. Supposons que $\alpha, \beta \in B$ et $\gamma = \alpha - \beta \in R$. Quitte à prendre $-\gamma = \beta - \alpha$ à la place de γ, on peut aussi supposer que $\gamma \in R^+$, comme on le voit en écrivant :

$$\gamma \in R^- \Leftrightarrow \begin{cases} -\gamma \in R \\ \gamma \prec 0 \overset{\text{(II.1.a)}}{\Rightarrow} (-1) \times \gamma \succ (-1) \times 0 \Rightarrow -\gamma \succ 0. \end{cases}$$

Alors $\alpha = \beta + \gamma$ avec $\beta \in B \subset R^+$ et $\gamma \in R^+$, et α est la somme de deux racines positives ! C'est absurde puisque $\alpha \in B$.

III.3. Le produit scalaire

$$\langle v, v \rangle = \sum_{\substack{1 \leq i \leq r \\ r+1 \leq j \leq s}} \lambda_i \lambda_j \langle \alpha_i, \alpha_j \rangle = \sum_{\substack{1 \leq i \leq r \\ r+1 \leq j \leq s}} \frac{\lambda_i \lambda_j}{2} n_{\alpha_i,\alpha_j} ||\alpha_i||^2$$

est positif. Tous les termes λ_i, λ_j, $||\alpha_i||^2$ intervenant dans la somme sont positifs. Comme α_i et α_j appartiennent à B, II.2.b donne $n_{\alpha_i,\alpha_j} \leq 0$, et la somme précédente est négative. Le nombre $\langle v, v\rangle$, à la fois positif et négatif, ne peut être que nul, donc $\langle v, v\rangle = ||v||^2 = 0$ et $v = 0$. Ainsi

$$\lambda_1\alpha_1 + ... + \lambda_r\alpha_r = 0.$$

Par hypothèse $\lambda_i \geq 0$ et $\alpha_i \in B$ pour tout i. Ainsi $\alpha_i \in R^+$, et $\alpha_i \succ 0$. S'il existait un indice i tel que $\lambda_i > 0$, on aurait $\lambda_1\alpha_1 + ... + \lambda_r\alpha_r \succ 0$, ce qui est absurde. Donc $\lambda_i = 0$ pour tout $i \in \{1, ..., r\}$.
On montrerait de la même façon que $\lambda_i = 0$ pour tout $i \in \{r+1, ..., s\}$.

III.4. • *B est une partie génératrice de $\mathbb{R}^n$.* En effet :

⋆ R engendre $\mathbb{R}^n$,

⋆ $B \subset R$,

⋆ Tout élément de R est combinaison linéaire d'éléments de B. En effet, tout élément de R^+ est combinaison linéaire d'éléments de B d'après III.1.b, et si $\alpha \in R^-$, il suffit de voir que $-\alpha \in R^+$ pour constater que $-\alpha$ et α sont aussi des combinaisons linéaires d'éléments de B.

• *Montrons que B est une famille libre de $\mathbb{R}^n$.*
Soit $\lambda_1\alpha_1+...+\lambda_s\alpha_s = 0$ une combinaison linéaire nulle de s vecteurs de B, avec $(\lambda_1, ..., \lambda_s) \in \mathbb{R}^s$. Quitte à noter les coefficients autrement, on peut toujours supposer $\lambda_{r+1} \leq \lambda_{r+2} \leq ... \leq \lambda_s \leq 0 \leq \lambda_1 \leq \lambda_2 \leq ... \leq \lambda_r$. Dans ce cas

$$\lambda_1\alpha_1 + ... + \lambda_r\alpha_r = -\lambda_{r+1}\alpha_{r+1} - ... - \lambda_s\alpha_s,$$

et III.3 montre que tous les coefficients λ_i sont nuls.

• *Conclusion* : B est une partie libre et génératrice de $\mathbb{R}^n$, c'est donc une base de $\mathbb{R}^n$.

III.5. Voir FIG. 6.6.

Remarques : α) La question III.5 demande trop de temps pour être résolue de façon complète et en étant certain d'avoir tenu compte de tout ce qui précède. En situation de concours, il y a fort à parier qu'on décide de la sauter ou qu'on se borne à donner rapidement quatre dessins sans les vérifier : certains dessins seront justes, d'autres faux, et ce n'est pas grave tant qu'on avance dans le problème !

β) Pour trouver les bases B des systèmes de racines de $\mathbb{R}^2$ et obtenir la FIG. 6.6, on utilise les renseignements suivants :

- Les éléments de B sont dans R^+, donc dans la partie hachurée en II.2.a.
- Les éléments de B sont des racines simples, donc ne doivent pas s'écrire comme somme de deux racines positives.

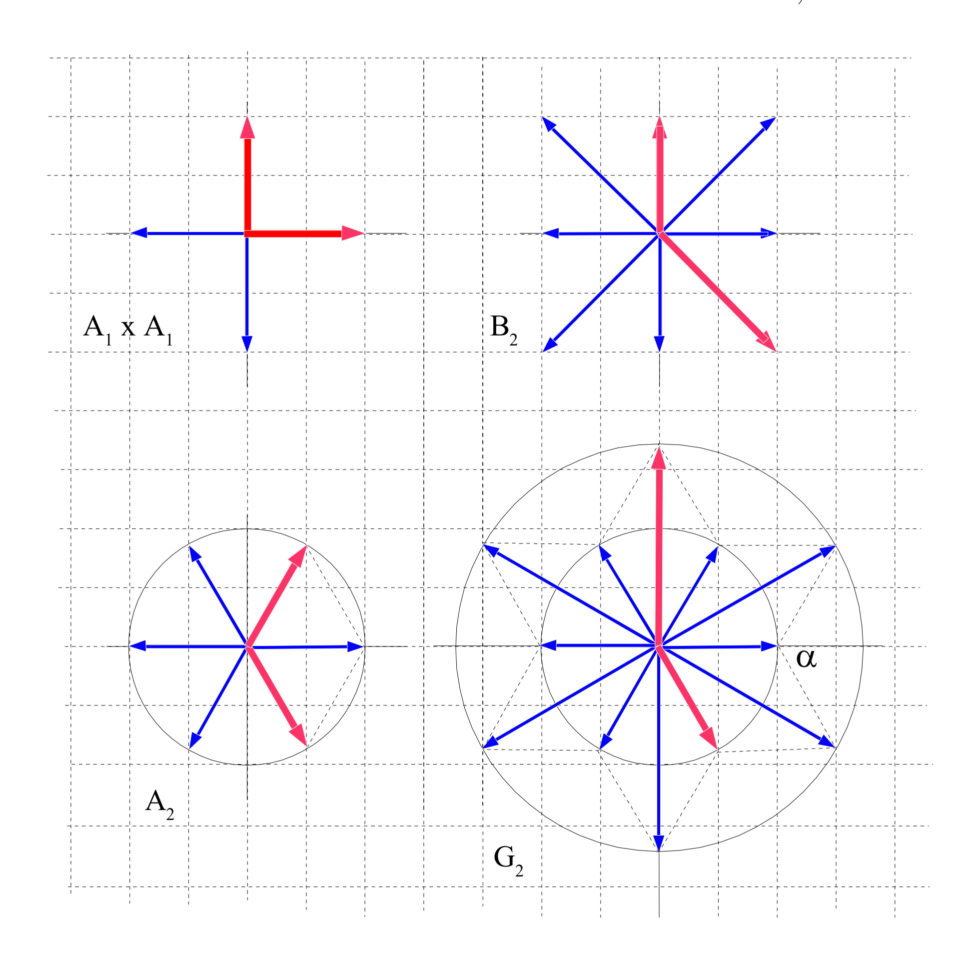


FIG. 6.6 – Cas particulier où $n = 2$

- Si $\alpha, \beta \in B$, alors $\alpha - \beta \notin R$ et $n_{\alpha,\beta} \leq 0$ d'après III.2.b. Cela impose d'avoir $\langle \alpha, \beta \rangle \leq 0$, autrement dit l'angle (α, β) est obtus.

Partie IV. GROUPE DE WEYL D'UN SYSTEME DE RACINES

IV.1. Comme cela a été dit dans la remarque préliminaire, s_a est la réflexion par rapport à l'hyperplan $(\mathbb{R}a)^\perp$ orthogonal à a.
L'application $f = \varphi \circ s_a \circ \varphi^{-1}$ étant linéaire comme composée de trois applications linéaires[1], montrer que f est la réflexion $s_{\varphi(a)}$ par rapport à l'hyperplan $(\mathbb{R}\varphi(a))^\perp$ revient simplement à vérifier que :

[1] Il est tout aussi facile d'affirmer que f est orthogonale comme composée de trois applications orthogonales, mais nous n'utiliserons pas cette information dans la suite de la démonstration.

(a) f transforme $\varphi(a)$ en son opposé,

(b) f laisse invariant tout vecteur de $(\mathbb{R}\varphi(a))^{\perp}$.

▷ Montrons (a) :

$$f(\varphi(a)) = \left(\varphi \circ s_a \circ \varphi^{-1}\right)(\varphi(a)) = \varphi\left[s_a(a)\right] = \varphi(-a) = -\varphi(a).$$

▷ Montrons (b) : Comme φ est une application orthogonale,

$$(\mathbb{R}\varphi(a))^{\perp} = (\varphi(\mathbb{R}a))^{\perp} = \varphi\left((\mathbb{R}a)^{\perp}\right).$$

Pour tout $x \in (\mathbb{R}\varphi(a))^{\perp}$, il existe donc $y \in (\mathbb{R}a)^{\perp}$ tel que $x = \varphi(y)$, et

$$f(x) = \left(\varphi \circ s_a \circ \varphi^{-1}\right)(\varphi(y)) = \varphi\left[s_a(y)\right] = \varphi(y) = x.$$

Remarques et compléments : On a rédigé la question IV.1 rapidement pour privilégier la vitesse, et c'est ce que l'on fera d'habitude en situation de concours. Mais il faut être capable de justifier complètement tout ce qui a été affirmé un peu rapidement : cela nous permet de mieux retenir ces résultats et de répondre à un jury d'oral si l'occasion se présente. Ne passons donc pas à côté de cet entraînement !

⇝ *Première propriété admise* : $\mathbb{R}\varphi(a) = \varphi(\mathbb{R}a)$.
L'automorphisme φ transforme la droite vectorielle $\mathbb{R}a$ en une droite vectorielle (un sous-espace vectoriel de même dimension que $\mathbb{R}a$) dirigée par $\varphi(a)$ (qui n'est pas nul puisque a n'est pas nul). Donc $\mathbb{R}\varphi(a) = \varphi(\mathbb{R}a)$. Une autre façon de répondre est de dire que $\varphi(\mathbb{R}a)$ est décrit par les vecteurs $\varphi(\lambda a) = \lambda\varphi(a)$ lorsque λ décrit $\mathbb{R}$, et que l'on reconnaît la droite vectorielle engendrée par $\varphi(a)$.

⇝ *Seconde propriété admise* : $(\varphi(\mathbb{R}a))^{\perp} = \varphi\left((\mathbb{R}a)^{\perp}\right)$.
Si $\varphi \in \mathrm{O}(\mathbb{R}^n)$ et si V est un sous-espace vectoriel de $\mathbb{R}^n$, on vérifie que l'on a toujours $(\varphi(V))^{\perp} = \varphi\left(V^{\perp}\right)$. En effet,

$$\begin{cases} \dim\varphi\left(V^{\perp}\right) = \dim V^{\perp} = n - \dim V \\ \dim(\varphi(V))^{\perp} = n - \dim\varphi(V) = n - \dim V, \end{cases}$$

donc $\dim\varphi\left(V^{\perp}\right) = \dim(\varphi(V))^{\perp}$. L'égalité annoncée sera donc assurée si l'on prouve l'inclusion $\varphi\left(V^{\perp}\right) \subset (\varphi(V))^{\perp}$. C'est facile : si $x \in V^{\perp}$ et $y \in \varphi(V)$, il existe $z \in V$ tel que $y = \varphi(z)$. Comme φ est orthogonale, elle conserve le produit scalaire et $\langle\varphi(x), y\rangle = \langle\varphi(x), \varphi(z)\rangle = \langle x, z\rangle = 0$. Donc

$$\forall x \in V^{\perp} \quad y \in \varphi(V) \qquad \langle\varphi(x), y\rangle = 0,$$

et cela signifie que $\varphi\left(V^{\perp}\right) \subset (\varphi(V))^{\perp}$.

Autre méthode : Un calcul direct donne aussi le résultat. En effet,

$$\begin{aligned}\left(\varphi \circ s_a \circ \varphi^{-1}\right)(x) &= \varphi\left[s_a\left(\varphi^{-1}(x)\right)\right] \\ &= \varphi\left[\varphi^{-1}(x) - 2\frac{\left\langle a, \varphi^{-1}(x)\right\rangle}{||a||^2}a\right] \\ &= x - 2\frac{\left\langle a, \varphi^{-1}(x)\right\rangle}{||a||^2}\varphi(a) \\ &= x - 2\frac{\langle \varphi(a), x\rangle}{||\varphi(a)||^2}\varphi(a) \quad = \quad s_{\varphi(a)},\end{aligned}$$

l'avant-dernière égalité étant vraie puisque φ conserve le produit scalaire.

IV.2. **Première méthode** : Toutes les symétries s_a qui engendrent W sont involutives. Les éléments de W sont donc de la forme $s_{a_1} \circ s_{a_2} \circ ... \circ s_{a_m}$, où m est un entier naturel quelconque (si $m = 0$, on pose $s_{a_1} \circ s_{a_2} \circ ... \circ s_{a_m} = Id$ par convention). Par hypothèse R est de cardinal fini $|R|$. On aura donc montré que W est fini si l'on montre que :

Lemme W : Tout élément de W s'écrit $s_{a_1} \circ s_{a_2} \circ ... \circ s_{a_m}$
avec $m \leq |R|$ et $a_1, ..., a_m \in R$.

Preuve du Lemme W : Si $f = s_{a_1} \circ s_{a_2} \circ ... \circ s_{a_m}$ avec $m > |R|$, on montre que f est la composée de moins de $m - 1$ symétries s_α où $\alpha \in R$.
En effet, l'hypothèse $m > |R|$ montre qu'il existe deux réflexions identiques parmi les m réflexions s_{a_i}. Par exemple $s_{a_i} = s_{a_j}$ pour deux indices i, j tels que $i < j$, et l'on peut alors supprimer l'une des applications dans le "tronçon" :

$$\tau = s_{a_i} \circ s_{a_{i+1}} \circ ... \circ s_{a_j}.$$

La question précédente donne $s_{\varphi(a)} = \varphi \circ s_a \circ \varphi^{-1}$, ou encore

$$s_{s_b(a)} \circ s_b = s_b \circ s_a$$

en appliquant la formule avec $\varphi = s_b$. Par hypothèse, $s_b(a)$ appartient à R quels que soient $a, b \in R$. Cette "pseudo-commutativité" nous permet de rapprocher s_{a_i} de s_{a_j} dans τ, et de les annihiler puisque $s_{a_i} \circ s_{a_j} = Id$.
En effet :

$$\begin{aligned}\tau &= s_{a_i} \circ s_{a_{i+1}} \circ ... \circ s_{a_j} \\ &= s_{s_{a_i}(a_{i+1})} \circ s_{a_i} \circ s_{a_{i+2}} \circ ... \circ s_{a_j} \\ &= s_{s_{a_i}(a_{i+1})} \circ s_{s_{a_i}(a_{i+2})} \circ s_{a_i} \circ ... \circ s_{a_j} \\ &= ... \\ &= s_{s_{a_i}(a_{i+1})} \circ s_{s_{a_i}(a_{i+2})} \circ ... \circ s_{s_{a_i}(a_{j-1})} \circ s_{a_i} \circ s_{a_j}\end{aligned}$$

soit $\tau = s_{s_{a_i}(a_{i+1})} \circ s_{s_{a_i}(a_{i+2})} \circ ... \circ s_{s_{a_i}(a_{j-1})}$ comme on le désirait !

Seconde méthode : L'application

$$i: \begin{array}{ccc} W & \to & \mathfrak{S}(R) \\ s & \mapsto & s \end{array}$$

est un morphisme de groupes injectif de W dans le groupe $\mathfrak{S}(R)$ des permutations de R. Comme R est fini, $\mathfrak{S}(R)$ aussi et W, isomorphe à un sous-groupe de $\mathfrak{S}(R)$, est fini.

IV.3.a. • D'après III.1.b, tout élément de R^+ est combinaison linéaire d'éléments de B à coefficients dans $\mathbb{N}$. On sait aussi que B est une base de $\mathbb{R}^n$ (III.4). Si l'on note $B = (b_1, ..., b_n)$, il existe donc n entiers naturels λ_i tels que $\alpha = \lambda_1 b_1 + ... + \lambda_n b_n$, et

$$\langle \alpha, \alpha \rangle = \sum_{i=1}^{n} \lambda_i \ \langle b_i, \alpha \rangle .$$

Le vecteur α n'est pas nul puisqu'appartient à R, donc $\langle \alpha, \alpha \rangle > 0$. Les λ_i étant positifs, tous les réels $\langle b_i, \alpha \rangle$ intervenant dans la somme précédente ne peuvent pas être ≤ 0, sinon l'on aurait $\langle \alpha, \alpha \rangle = \sum_{i=1}^{n} \lambda_i \ \langle b_i, \alpha \rangle \leq 0$, ce qui est absurde. Il existe donc $i_0 \in \{1, ..., n\}$ tel que $\langle b_{i_0}, \alpha \rangle > 0$, et il ne reste plus qu'à poser $\beta = b_{i_0}$.

• On en déduit $n_{\beta,\alpha} = 2\dfrac{\langle \beta, \alpha \rangle}{||\beta||^2} > 0$, puis $\beta - \alpha \in R$ et $\alpha - \beta \in R$ d'après la question III.2.a.

Comme $\alpha \neq \beta$ (car $\alpha \in R^+ \backslash B$), on peut écrire

$$\begin{aligned} \alpha - \beta \notin R^+ &\Rightarrow \alpha - \beta \in R^- \\ &\Rightarrow \beta - \alpha \in R^+ \\ &\Rightarrow \exists \alpha, \gamma \in R^+ \quad \beta = \alpha + \gamma, \end{aligned}$$

et la conclusion obtenue est fausse puisque β appartient à B. L'hypothèse $\alpha - \beta \notin R^+$ est donc fausse, donc $\alpha - \beta \in R^+$.

IV.3.b. Notons toujours $B = (b_1, ..., b_n)$ et $\alpha = \lambda_1 b_1 + ... + \lambda_n b_n$, où les coefficients λ_1, ..., λ_n appartiennent à $\mathbb{N}$. Quitte à changer l'ordre des vecteurs de la base B, on peut supposer $b_1 = \beta$. Alors

$$s_\beta(\alpha) = \alpha - n_{\beta,\alpha}\beta = (\lambda_1 - n_{\beta,\alpha})\, b_1 + ... + \lambda_n b_n.$$

On sait que $\alpha \in R$ entraîne $s_\beta(\alpha) \in R$. D'après III.1.b, on sait aussi que les éléments de R sont de deux sortes :

- ceux de R^+, qui s'écrivent $\mu_1 b_1 + ... + \mu_n b_n$ avec $\mu_1, ..., \mu_n \in \mathbb{N}$,
- ceux de R^-, qui s'écrivent $\mu_1 b_1 + ... + \mu_n b_n$ avec $\mu_1, ..., \mu_n \in \mathbb{Z}_-$.

Montrer que $s_\beta(\alpha)$ appartient à R^+ revient donc à prouver que l'une au moins de ses coordonnées dans la base B est strictement positive. Pour cela, nous allons montrer l'existence d'un indice $i \in \{2, ..., n\}$ tel que $\lambda_i \neq 0$. La i-ième coordonnée de $s_\beta(\alpha)$ dans B sera alors strictement positive, et l'on aura bien $s_\beta(\alpha) \in R^+$.
Raisonnons par l'absurde : si $\lambda_2 = ... = \lambda_n = 0$, alors $\alpha = \lambda_1 b_1$, et puisque deux racines de R sont proportionnelles si et seulement si elles sont égales ou opposées, on obtient $\alpha = \pm b_1 = \pm \beta$.
Comme $\alpha \neq \beta$, on en déduit $\alpha = -\beta$, mais c'est impossible puisque $\alpha \in R^+$ et $-\beta \in R^-$.

IV.4.a. Supposons par l'absurde que $R^+ \subsetneq S$. On peut alors définir le minimum de $R^+ \backslash S$ pour la relation d'ordre $\preceq$, soit :

$$\alpha = \text{Min}\left(R^+ \backslash S\right).$$

Si α appartenait à B, comme $Id \in W_B$, on obtiendrait $\alpha = Id(\alpha) \in S$, ce qui est absurde. Donc $\alpha \notin B$ et l'on peut appliquer IV.3.a : il existe $\beta \in B$ tel que $n_{\beta,\alpha} > 0$ et $\alpha - \beta \in R^+$. Par suite

$$s_\beta(\alpha) = \alpha - n_{\beta,\alpha}\beta \prec \alpha.$$

La question IV.3.b montre que $s_\beta(\alpha) \in R^+$, et l'inégalité précédente impose d'avoir $s_\beta(\alpha) \in S$ (pour ne pas contredire la définition de α). Il existe donc $w \in W_B$ et $\gamma \in B$ tels que $s_\beta(\alpha) = w(\gamma)$.
Comme s_β est involutive, $\alpha = (s_\beta \circ w)(\gamma)$, et comme $s_\beta \circ w \in W_B$, on en déduit $\alpha \in S$, ce qui est absurde ! Donc $R^+ \backslash S = \varnothing$ et $R^+ \subset S$.

Remarque stratégique : Adeptes du surnaturel, traitez cette question en 5 ou 10 minutes. Quant aux autres, réfléchissez 5 minutes, tout au plus, sur cette question, puis passez à autre chose si vous êtes en situation de concours, ou lisez la solution si vous êtes en situation d'entraînement.

Le pauvre correcteur que je suis aurait immédiatement sauté les questions IV.3 et IV.4 en situation de concours, pour gagner des points dans les parties V ou VI.

La question IV.4 est trop difficile pour être traitée en temps limité, voire pour être traitée tout court. Elle est par contre facile à comprendre lorsqu'on lit la solution. Ce n'est pas une question de cours, ce n'est pas la mise en oeuvre d'une méthode classique. Il s'agit d'une délicate mise au point d'un raisonnement permettant d'aller d'une hypothèse à une conclusion. La méthode employée consiste à utiliser les hypothèses pour aboutir à une absurdité. D'une certaine manière, on se trouve dans un labyrinthe ou l'on doit "pousser des portes", puis encore et encore, jusqu'à obtenir une contradiction tangible. Ce type de recherche (où l'on gigote dans un labyrinthe) peut fonctionner en 5 minutes comme en de nombreuses années. Il est hors de question de subordonner sa réussite aux épreuves à ce type d'exercice aléatoire !

J'insiste. Deux cas se présentent :

▷ *En situation de concours*, il s'agit de ne *PAS HYPOTHEQUER* le reste du problème en s'acharnant à résoudre une question comme la question IV.4. Au bout de 5 minutes (ou moins) de recherches infructueuses (et sans avoir de piste relativement fiable à suivre), *IL FAUT S'INQUIETER* et *COUPER !* Il faut s'arrêter pour passer à autre chose, admettre la question et utiliser son temps pour avancer dans le problème, quel que soit l'endroit où l'on va pouvoir avancer.

Une année de préparation derrière soi, et rater stupidement son épreuve en s'acharnant sur une petite question infaisable ? Non !

Et ne soyons pas trop triste : disons-nous mentalement que nous pourrons revenir sur cette question lorsqu'on aura épuisé toutes les questions du problème dont nous détenons la solution. Voilà une bonne façon de réagir en concours !

▷ *En situation d'entraînement*, on cherchera cette question pendant 5 minutes (moins si l'ennui vient rapidement : le but n'est pas de se décourager, mais de fourbir ses armes !), puis on considérera que son travail consiste à LIRE ATTENTIVEMENT la solution en la comprenant.

Comprendre parfaitement la solution, arriver à justifier chacune des affirmations lues, comprendre les mécanismes et examiner les outils utilisés : cela s'appelle "faire des mathématiques" et permet de "faire des progrès". C'est exactement le but de tout notre entraînement.

Et puis, rassurons-nous : on aura tout le temps de s'entraîner à

la recherche et à la rédaction en utilisant d'autres parties du problème ou d'autres exercices adaptés.

IV.4.b. • *Montrons l'inclusion $R \subset S$.*
On a déjà $R^+ \subset S$ d'après IV.4.a, et il s'agit de vérifier que $R^- \subset S$.
Si $\alpha \in R^-$, alors $-\alpha = s_\alpha(\alpha) \in R^+ \subset S$ donc il existe $w \in W_B$ et $\beta \in B$ tels que $-\alpha = w(\beta)$. On en déduit

$$\alpha = w(-\beta) = (w \circ s_\beta)(\beta) \in S$$

car $w \circ s_\beta \in W_B$.

• *Montrons l'inclusion $S \subset R$.*
Un élément quelconque de S s'écrit $w(\alpha)$ avec $w \in W_B$ et $\alpha \in B$. A fortiori $w \in W$ et $\alpha \in R$, donc $w(\alpha) \in R$ (puisque R est un système de racines, et que w est la composée d'un nombre fini de réflexions s_γ où $\gamma \in R$).

IV.4.c. On a $W_B \subset W$. Pour conclure à $W = W_B$, il s'agit de montrer l'inclusion réciproque $W \subset W_B$.
Le groupe W étant engendré par les réflexions s_α où α décrit R, montrer que $W \subset W_B$ revient à prouver que s_α appartient à W_B pour tout $\alpha \in R$.
Soit $\alpha \in R$. Puisque $R = S$, il existe $w \in W_B$ et $\beta \in B$ tels que $\alpha = w(\beta)$. La question IV.1 permet alors d'écrire

$$s_\alpha = s_{w(\beta)} = w \circ s_\beta \circ w^{-1}$$

et de déduire que s_α appartient au groupe W_B comme composée de trois éléments de ce groupe.

Partie V. GROUPES DIEDRAUX

V.1.a. L'énoncé ne précise pas si le polygone régulier $\mathcal{P}_p$ est convexe ou non. En fait, un polygone est ici considéré comme un ensemble de sommets, et cette définition "sommaire" m'autorise à supposer que $M_0M_1...M_{p-1}$ est un polygone régulier <u>convexe</u> (quitte à réindexer les sommets M_k dans le bon ordre), ce que je m'empresse de faire.

Le centre O de $\mathcal{P}_p$ est par définition, à la fois :

- l'isobarycentre des points M_0, M_1, ..., M_{p-1} ;
- le centre du cercle circonscrit à $\mathcal{P}_p$.

[Voilà l'occasion de travailler la leçon d'oral sur les polygones réguliers, en [18] Chap. 9. Cette leçon est importante pour les écrits comme pour les oraux des concours !]

Dans le repère orthonormal direct $\mathcal{R}$ d'origine O tel que M_0 soit d'affixe 1, l'affixe de M_k est $e^{ik2\pi/p}$.
Dans la suite :

- j'identifie les points de E et leurs affixes dans $\mathcal{R}$;

- j'écris $M_u = M_v$ dès que u et v sont des entiers congrus modulo p (un même sommet de $\mathcal{P}_p$ peut donc avoir des noms différents).

► La rotation ρ laisse $\mathcal{P}_p$ globalement invariant. En effet, l'expression complexe de ρ étant $\rho(z) = e^{i2\pi/p}z$, on obtient $\rho(M_k) = e^{i(k+1)2\pi/p} = M_{k+1}$ pour tout k. Le sous-groupe cyclique $\langle\rho\rangle = \{Id, \rho, ..., \rho^{p-1}\}$ engendré par ρ est donc inclus dans C_p.

► Réciproquement, si f appartient à C_p, alors f est affine et conserve la partie $\{M_0, M_1, ..., M_{p-1}\}$, donc conserve aussi l'isobarycentre de cette partie, et l'on a $f(O) = O$.
Puisque f est un déplacement, ce ne peut être qu'une rotation de centre O. Par hypothèse, il existe $k \in \{0, 1, ..., p-1\}$ tel que $f(M_0) = M_k = \rho^k(M_0)$. Comme une rotation de centre O est parfaitement déterminée par l'image d'un point (autre que O), on obtient $f = \rho^k$, donc $f \in \langle\rho\rangle$.
On vient de montrer l'inclusion $C_p \subset \langle\rho\rangle$.

► Finalement

$$C_p = \langle\rho\rangle = \{Id, \rho, ..., \rho^{p-1}\}.$$

Remarques :

α) Pour l'énoncé, $\mathcal{P}_p = \{M_0, M_1, ..., M_{p-1}\}$ est un ensemble de sommets, et "conserver $\mathcal{P}_p$" signifie "conserver la partie $\{M_0, M_1, ..., M_{p-1}\}$". Cela explique que nous puissions renommer les sommets pour que l'affixe de M_k soit égale à $e^{ik2\pi/p}$.

β) "Parcourir les sommets dans le sens direct", comme précisé dans l'énoncé, ne nous interdit pas d'avoir un polygone régulier étoilé. Mais encore une fois, ce qui nous importe ici, ce sont les sommets de $\mathcal{P}_p$ et non ses arêtes.

γ) Considérer le polygone régulier $\mathcal{P}_p$ comme une famille d'arêtes, c'est-à-dire poser

$$\mathcal{P}_p = \{[M_0M_1], ..., [M_{p-2}M_{p-1}], [M_{p-1}M_0]\},$$

et dire qu'une isométrie conserve $\mathcal{P}_p$ si et seulement si elle permute les arêtes $[M_kM_{k+1}]$, nous permettrait d'aboutir aux mêmes résultats dans toute cette partie, que $\mathcal{P}_p$ soit convexe ou non. Mais cela demanderait d'effectuer quelques vérifications supplémentaires.
Par exemple, avec cette définition de $\mathcal{P}_p$, et si l'on veut parcourir les sommets de $\mathcal{P}_p = M_0M_1...M_{p-1}$ en suivant ses arêtes (ce que l'on fait d'habitude), on doit définir le sommet M_k comme le point d'affixe $e^{ik\theta}$ (dans $\mathcal{R}$), où $\theta = s2\pi/p$

et où s désigne un entier premier avec p et compris entre 1 et $p-1$ ([18], Th. 127). On doit donc vérifier que la rotation ρ de centre O et d'angle $2\pi/p$ laisse encore $\mathcal{P}_p$ invariant, ce qui signifie ici que, pour tout $k \in \{0, ..., p-1\}$,

$$\rho\left([M_k M_{k+1}]\right) \in \{[M_0 M_1], ..., [M_{p-2} M_{p-1}], [M_{p-1} M_0]\}.$$

Pour cela on peut calculer $\rho(M_k) = e^{i2\pi/p} e^{ik\theta} = e^{i(2\pi/p+k\theta)}$ et chercher k' tel que $e^{i(2\pi/p+k\theta)} = e^{ik'\theta}$. On constate que :

$$e^{i(2\pi/p+k\theta)} = e^{ik'\theta} \quad \Leftrightarrow \quad \exists u \in \mathbb{Z} \quad 1 = \left(k' - k\right) s + up.$$

Comme u et p sont premiers entre eux, le Théorème de Bezout montre l'existence de deux entiers k_0 et u_0 tels que $1 = k_0 s + u_0 p$, et il suffit de choisir $k' = k + k_0$ pour obtenir $\rho(M_k) = M_{k'} = M_{k+k_0}$.
L'image de l'arête $[M_k M_{k+1}]$ par ρ est donc l'arête $[M_{k+k_0} M_{k+k_0+1}]$.

V.1.b. Dans toute la suite de la Partie V, je pose $\theta = 2\pi/p$. La réflexion σ par rapport à (OM_0) laisse $\mathcal{P}_p$ invariant. En effet, son expression complexe est $\sigma(z) = \overline{z}$, et $\sigma(M_k) = \overline{e^{ik\theta}} = e^{-ik\theta} = e^{i(p-k)\theta} = M_{p-k}$ pour tout k.

V.1.c. Soit A_p l'ensemble des antidéplacements de D_{2p}. Clairement

$$D_{2p} = C_p \bigsqcup A_p$$

et $\sigma \in A_p$. On montre que l'application

$$\Psi : \begin{array}{ccc} C_p & \rightarrow & A_p \\ f & \mapsto & f \circ \sigma \end{array}$$

est bijective. Tout d'abord, Ψ est bien définie car la composée d'un déplacement et d'un antidéplacement est un antidéplacement, et que la composée de deux isométries qui conservent $\mathcal{P}_p$ conserve encore $\mathcal{P}_p$. Ensuite Ψ est injective puisque $f \circ \sigma = g \circ \sigma$ entraîne $f = g$. Enfin tout antidéplacement g de A_p s'écrit sous la forme $g = f \circ \sigma$ avec $f = g \circ \sigma \in C_p$. Donc Ψ est surjective.
Puisque Ψ est bijective, les cardinaux de C_p et A_p sont égaux et l'on a même : $|C_p| = |A_p| = p$. Tout élément de A_p s'écrit de façon unique $f \circ \sigma$ avec $f \in C_p$, donc sous la forme $\rho^k \circ \sigma$ avec $k \in \{0, 1, ..., p-1\}$. Finalement

$$\begin{aligned} D_{2p} &= C_p \bigsqcup A_p \\ &= \{Id, \rho, ..., \rho^{p-1}\} \bigsqcup \{\sigma, \rho \circ \sigma, ..., \rho^{p-1} \circ \sigma\} \\ &= \{\rho^i \circ \sigma^j \,/\, i \in \{0, 1, ..., p-1\} \text{ et } j \in \{0, 1\}\}. \end{aligned}$$

Remarque : Cette question est une ROC[2] et il faut savoir y répondre. C'est pour ces questions qu'on s'entraîne avant un concours ! C'est la question n°3 du jury dans l'exposé sur les polygones réguliers ([18], § 9.2.2) et on la retrouve dans la Section 14.1.1 du cours de géométrie où sont rassemblés des résultats fondamentaux avec lesquels on doit être familiarisé (voir [15], Th. 225).

V.1.d. L'application $f = \sigma \circ \rho^k \circ \sigma$ est un déplacement laissant $\mathcal{P}_p$ invariant (comme composée de deux antidéplacements et d'un déplacement laissant $\mathcal{P}_p$ invariant). C'est donc l'une des rotations de C_p. Pour la déterminer, il suffit de déterminer $f(M_0)$. On a

$$f(M_0) = \sigma[\rho^k(\sigma(M_0))] = \sigma[\rho^k(M_0)] = \sigma(M_k) = M_{p-k}$$

(on a montré que $\sigma(M_k) = M_{p-k}$ en V.1.b), donc $f(M_0) = \rho^{p-k}(M_0)$. Les rotations f et ρ^{p-k} sont de même centre O et amènent M_0 sur M_{p-k}. Elles sont donc égales. Ainsi $\sigma \circ \rho^k \circ \sigma = \rho^{p-k}$.

V.2.a. s est d'ordre 2, donc $s^{-1} = s$ et $s' = sr$. Tout élément de G s'écrit sous la forme $x = s^{\alpha_1} s'^{\beta_1} ... s^{\alpha_m} s'^{\beta_m}$ où $m \in \mathbb{N}$ et $\alpha_1, \beta_1, ..., \alpha_m, \beta_m \in \mathbb{Z}$ (en posant par convention $x = e$ si $m = 0$), donc s'écrit aussi sous la forme

$$x = s^{\alpha_1}(sr)^{\beta_1} ... s^{\alpha_m}(sr)^{\beta_m}$$

d'un produit de puissances de s et de r. Le groupe G est donc inclus dans le sous-groupe $\langle r, s\rangle$ de G engendré par r et s. Comme l'inclusion $\langle r, s\rangle \subset G$ est triviale, on en déduit $G = \langle r, s\rangle$.

Remarque : Dans l'écriture de x sous la forme $x = s^{\alpha_1} s'^{\beta_1} ... s^{\alpha_m} s'^{\beta_m}$, on peut supposer que les α_i et β_i appartiennent à $\mathbb{N}$ car s et s' sont involutives.

V.2.b. • On a $sr = s(ss') = s' = (s's)s = (ss')^{-1}s = r^{-1}s$.

• On vérifie que $sr^k = r^{p-k}s$ pour tout $k \in \mathbb{N}$ en raisonnant par récurrence sur k.
- Si $k = 0$, la propriété est triviale (en effet $sr^0 = s = r^{p-0}s$ puisque $r^p = e$).
- Si $k = 1$, on vient de voir que $sr = r^{-1}s$.
- Si elle est vraie au rang k,

$$sr^{k+1} = sr^k r = r^{p-k} sr = r^{p-k} r^{-1} s = r^{p-(k+1)} s,$$

donc elle est encore vraie au rang $k+1$.

• Posons $\Lambda = \{r^i s^j \,/\, i \in \{0, 1, ..., p-1\}$ et $j \in \{0, 1\}\}$. On a bien sûr $\Lambda \subset G$. Réciproquement, tout élément de $G = \langle r, s\rangle$ s'écrit comme un produit

[2] Restitution Organisée de Connaissances.

fini d'éléments de la forme r^α ou s^β avec $\alpha, \beta \in \mathbb{Z}$. Un tel produit pourra toujours s'écrire sous la forme $r^\alpha s^\beta$ en utilisant autant de fois que nécessaire la "pseudo-commutativité" $sr^k = r^{p-k}s$ pour rassembler tous les r à gauche et tous les s à droite.
Si l'on écrit les divisions euclidiennes de α par p, et de β par 2, on obtient

$$\begin{cases} \alpha = pq + i \quad \text{avec } i \in \{0, 1, ..., p-1\} \\ \beta = 2q' + j \quad \text{avec } j \in \{0, 1\}, \end{cases}$$

d'où $r^\alpha\, s^\beta = (r^p)^q r^i\, (s^2)^{q'} s^j = r^i s^j$. Tout élément de G s'écrit donc sous la forme voulue. En conclusion

$$G = \{r^i s^j \,/\, i \in \{0, 1, ..., p-1\} \text{ et } j \in \{0, 1\}\}.$$

Autre méthode : On montre que Λ est un sous-groupe de G qui contient r et s. Comme le groupe G est engendré par r et s, on en déduit $G \subset \Lambda$, donc $G = \Lambda$.
Il est évident que Λ est inclus dans G et contienne r et s. Il s'agit donc seulement de vérifier que Λ est un sous-groupe de G :

- C'est une partie non vide (elle contient r et s).
- Le produit de deux éléments de Λ reste dans Λ car

$$\begin{cases} r^i r^{i'} = r^{i+i'} \\ r^i s r^{i'} s = r^i r^{p-i'} s^2 = r^{p+i-i'} \\ r^i s r^{i'} = r^i r^{p-i'} s = r^{p+i-i'} s \\ r^i r^{i'} s = r^{i+i'} s, \end{cases}$$

et puisque, dans ces expressions, les exposants de $r^{p+i-i'}$ et $r^{i+i'}$ peuvent toujours être ramenés à des entiers compris entre 0 et $p-1$ en utilisant une division euclidienne par p, comme on l'a déjà fait plus haut.

- L'inverse d'un élément de Λ reste dans Λ. En effet

$$\begin{cases} (r^0)^{-1} = e^{-1} = e, \\ (r^i)^{-1} = r^{p-i} \quad \text{avec } 1 \leq p-i \leq p-1, \text{ si } i \in \{1, ..., p-1\}, \\ (r^0 s)^{-1} = s, \\ (r^i s)^{-1} = s r^{-i} = s r^{p-i} = r^{p-(p-i)} s = r^i s \quad \text{si } i \in \{1, ..., p-1\}. \end{cases}$$

V.2.c. • Supposons par l'absurde que $s = r^k$ pour un certain $k \in \mathbb{N}$. Alors $r^i s^j = r^{i+kj}$ et G est engendré par r. G est donc un groupe cyclique d'ordre p, et à ce titre c'est un groupe abélien.
N'oublions pas que $G = \langle s, s' \rangle$ est aussi engendré par deux éléments d'ordre 2. Puisque G est commutatif, ses seuls éléments seront donc e, s, s' et ss', et

nous reconnaissons le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Un tel groupe n'est pas cyclique, d'où l'absurdité !

Autre façon de conclure : On montre encore que G est cyclique (donc commutatif) et engendré par r. Comme $r^2 = (ss')^2 = s^2 s'^2 = e$, on en déduit $G = \{e, r\}$, ce qui est absurde puisque G contient au moins les trois éléments e, s et s'.

• Les éléments e, r, ..., r^{p-1} sont deux à deux distincts. Il en va de même de s, $r \circ s$, ..., $r^{p-1} \circ s$ puisque si $i, j \in \{0, ..., p-1\}$,

$$r^i \circ s = r^j \circ s \quad \Rightarrow \quad r^i = r^j \quad \Rightarrow \quad i = j.$$

Aucun élément de la forme r^i ne peut s'écrire sous la forme $r^j \circ s$ (avec $i, j \in \{0, ..., p-1\}$) puisque

$$r^i = r^j \circ s \quad \Rightarrow \quad r^{i-j} = s \quad \Rightarrow \quad \exists k \in \mathbb{N} \quad s = r^k,$$

et qu'il n'existe aucun entier k tel que $s = r^k$. Finalement, G est formé des $2p$ éléments distincts e, r, ..., r^{p-1}, s, $r \circ s$, ..., $r^{p-1} \circ s$.

V.2.d. Pour tout $(i, j) \in \{0, 1, ..., p-1\} \times \{0, 1\}$, posons $\xi\left(r^i s^j\right) = \rho^i \circ \sigma^j$. On définit ainsi une application

$$\xi : \begin{array}{ccc} G & \rightarrow & D_{2p} \\ r^i s^j & \mapsto & \rho^i \circ \sigma^j, \end{array}$$

et l'on montre que c'est un isomorphisme de groupes. Avant de le vérifier, notons que l'on a aussi $\xi\left(r^i s^j\right) = \rho^i \circ \sigma^j$ pour tout $(i, j) \in \mathbb{Z} \times \{0, 1\}$ puisque r et ρ sont d'ordre p.

• C'est un homomorphisme car les formules des questions V.1.d et V.2.b sont du même type. Plus précisément :

$$\begin{cases} \xi(r^i r^{i'}) = \xi(r^{i+i'}) = \rho^{i+i'} = \rho^i \circ \rho^{i'} = \xi(r^i) \circ \xi(r^{i'}), \\ \xi(r^i (r^{i'} s)) = \xi(r^{i+i'} s) = \rho^{i+i'} \circ \sigma = \rho^i \circ (\rho^{i'} \circ \sigma) = \xi(r^i) \circ \xi(r^{i'} s), \\ \xi((r^i s) r^{i'}) = \xi(r^{i+p-i'} s) = \rho^{i+p-i'} \circ \sigma = (\rho^i \circ \sigma) \circ \rho^{i'} = \xi(r^i s) \circ \xi(r^{i'}), \\ \xi((r^i s)(r^{i'} s)) = \xi(r^{i+p-i'}) = \rho^{i+p-i'} = (\rho^i \circ \sigma) \circ (\rho^{i'} \circ \sigma) = \xi(r^i s) \circ \xi(r^{i'} s). \end{cases}$$

• ξ est surjective par construction.

• ξ est une application surjective entre deux ensembles finis de même cardinal $2p$, c'est donc une bijection d'après le Lemme suivant[3].

[3]Ce Lemme n'est ni à énoncer, ni à démontrer si l'on est en situation de concours. Il y a d'autres questions à traiter dans le problème. Il est néanmoins toujours conseillé de se poser des questions supplémentaires pendant son entraînement pour mieux connaître son sujet et pouvoir répondre à des questions du jury à l'oral du concours.

Lemme : Une application surjective $f : E \to F$ entre deux ensembles finis de même cardinal est une bijection.

Preuve du Lemme : L'application $g : F \to E$ qui à $y \in F$ associe l'un des antécédents de y par f (axiome du choix) vérifie $f \circ g = Id_F$, elle est donc injective ([20], exercice 1). De $|g(F)| = |F| = |E|$ et $g(F) \subset E$ on déduit $g(F) = E$, et g est bijective. Finalement $f = g^{-1}$ est la bijection réciproque de g. ■

Remarque : On aurait pu arguer du fait que tout élément de G s'écrit de manière unique sous la forme $r^i s^j$ avec $(i, j) \in \{0, 1, ..., p-1\} \times \{0, 1\}$, pour démontrer que f est injective.

V.2.e. La question IV.4 montre que le groupe de Weyl d'un système de racines R de $\mathbb{R}^2$ est engendré par les réflexions s_α et s_β où $B = (\alpha, \beta)$ désigne une base de R associée à l'ordre sur $\mathbb{R}^2$).
W est un groupe fini, donc la rotation $\rho = s_\alpha \circ s_\beta$ est d'ordre fini p. La question V.2.d montre que W est isomorphe au groupe diédral D_{2p} d'indice p.
Pour déterminer p, il suffit de calculer l'ordre de ρ dans chacun des quatre cas de figures de la question III.5.

- Si $R = A_1 \times A_1$, $\rho = s_\alpha \circ s_\beta$ est la composée de deux réflexions d'axes orthogonaux, c'est donc $-Id$. Dans ce cas $p = 2$ et $W \simeq D_4$.

- Si $R = B_2$, ρ est la composée de deux réflexions dont les axes font un angle de $\pm\pi/4$. L'ordre de ρ est alors $p = 4$, et $W \simeq D_8$.

- Si $R = A_2$, ρ est la composée de deux réflexions par rapport à des axes faisant des angles polaires de $\pi/3 + \pi/2 = 5\pi/6$ et $-\pi/3 + \pi/2 = \pi/6$. L'angle entre ces droites est donc mesuré par $5\pi/6 - \pi/6 = 2\pi/3$ (au signe près), et ρ est une rotation d'angle $\pm 4\pi/3$. Par suite $p = 3$ et $W \simeq D_6$.

- Si $R = G_2$, les axes de s_α et s_β font un angle de $\pm\pi/6$, donc ρ est d'angle $\pm\pi/3$ et d'ordre $p = 6$. On obtient encore $W \simeq D_{12}$.

Partie VI. CHAMBRES DE WEYL

VI.1. Les hyperplans P_α sont des fermés de $\mathbb{R}^n$ (P_α est le noyau d'une forme linéaire l_α sur $\mathbb{R}^n$, et l_α est continue car l'espace vectoriel normé $\mathbb{R}^n$ est de dimension finie. Ainsi $P_\alpha = l_\alpha^{-1}(\{0\})$ est fermé comme l'image réciproque d'un fermé par une application continue). La partie

$$\Omega = \mathbb{R}^n \backslash \bigcup_{\alpha \in R} P_\alpha = \bigcap_{\alpha \in R} (\mathbb{R}^n \backslash P_\alpha)$$

est l'intersection finie des ouverts $\mathbb{R}^n \backslash P_\alpha$. Il s'agit donc d'un ouvert.

VI.2. Soit $x \in C$. Il existe une chambre de Weyl C_1 contenant x. Comme $C \subset \Omega$, on a la réunion disjointe

$$C = (C \cap C_1) \bigsqcup (C \cap \Omega \backslash C_1) . \quad (*)$$

Comme C_1 est ouvert, l'intersection $C \cap C_1$ est un ouvert de C. Comme Ω est réunion disjointe des chambres de Weyl, qui sont des ouverts, $\Omega \backslash C_1$ est un ouvert de $\mathbb{R}^n$, donc $C \cap \Omega \backslash C_1$ est un ouvert de C.
$(*)$ montre que C est réunion disjointe de deux ouverts dont le premier n'est pas vide. Comme C est connexe, cela impose d'avoir $C \cap \Omega \backslash C_1 = \varnothing$, c'est-à-dire $C \subset C_1$.

VI.3. • Si $\alpha, \beta \in R$, $\gamma = s_\alpha(\beta)$ appartient à R, et puisque s_α est une application orthogonale,

$$s_\alpha(P_\beta) = s_\alpha((\mathbb{R}\beta)^\perp) = (s_\alpha(\mathbb{R}\beta))^\perp = (\mathbb{R}s_\alpha(\beta))^\perp = (\mathbb{R}\gamma)^\perp = P_\gamma$$

(voir remarque de la question IV.1).
L'application

$$\begin{array}{rccc} \zeta : & \{P_\gamma \,/\, \gamma \in R\} & \to & \{P_\gamma \,/\, \gamma \in R\} \\ & P_\beta & \mapsto & s_\alpha(P_\beta) \end{array}$$

est donc bien définie. Comme ζ est clairement injective, et comme $\{P_\gamma \,/\, \gamma \in R\}$ est un ensemble fini, on en déduit que ζ est bijective. Autrement dit s_α permute les hyperplans P_β $(\beta \in R)$.
Une application quelconque de W s'écrivant toujours comme la composée d'un nombre fini de réflexions s_α $(\alpha \in R)$, elle permutera les hyperplans P_β $(\beta \in R)$.

• Soient C une chambre de Weyl et $w \in W$. L'application linéaire w est continue (comme toutes les applications linéaires définies sur un espace vectoriel de dimension finie), donc transforme le connexe C en un connexe $w\,(C)$. Comme w permute les P_α et que C n'intercepte pas les hyperplans P_α, on aura $w\,(C) \subset \Omega$.
$w\,(C)$ est un connexe non vide de Ω, et la question VI.2 montre l'existence d'une chambre de Weyl C_1 telle que $w\,(C) \subset C_1$.
En recommençant avec w^{-1}, on montre aussi l'existence d'une chambre de Weyl C_2 telle que $w^{-1}\,(C_1) \subset C_2$. Comme $w\,(C) \subset C_1$, il existe $x \in C_1$ tel que $w^{-1}\,(x) \in C$. Dans ce cas $w^{-1}\,(x) \in C \cap C_2$, ce qui impose d'avoir $C = C_2$ puisque les chambres de Weyl forment une partition de Ω. Ainsi $w^{-1}\,(C_1) \subset C$, donc $C_1 \subset w\,(C)$.
En conclusion $w\,(C) = C_1$ et w permute les chambres de Weyl.

VI.4.a. Le groupe W étant fini, la partie $\{||x_1 - w'(x_2)|| \,/\, w' \in W\}$ est finie, non vide et incluse dans $\mathbb{R}$, donc possède un plus petit élément. Il existe donc $w \in W$ tel que $||x_1 - w(x_2)|| = \mathrm{Min}\{||x_1 - w'(x_2)|| \,/\, w' \in W\}$.

VI.4.b. • Il suffit de montrer que I n'intercepte aucun hyperplan P_α pour pouvoir conclure à $I \subset C_1$. En effet, si I n'intercepte aucun P_α, on a $I \subset \Omega$. Comme I est un intervalle, c'est un connexe, et VI.2 montre qu'il est inclus dans une chambre de Weyl. Comme $x_1 \in I \cap C_1$, on conclut bien à $I \subset C_1$.

• Montrons donc que I n'intercepte aucun hyperplan P_α, en raisonnant par l'absurde : supposons qu'il existe $\alpha \in R$ tel que $I \cap P_\alpha \neq \varnothing$. L'intervalle $I = [x_1; w(x_2)]$ coupe P_α en z, et il existe $t_0 \in [0,1]$ tel que

$$z = t_0 x_1 + (1 - t_0) w(x_2).$$

On ne peut pas avoir $t_0 = 0$ (sinon $w(x_2) \in P_\alpha$, mais w permute les chambres de Weyl, donc transforme $x_2 \in C_2$ en $w(x_2)$ qui appartient à une chambre de Weyl, pas à une frontière P_α !) ou encore $t_0 = 1$ (car $x_1 \in C_1$ et $C_1 \cap P_\alpha = \varnothing$). Ainsi

$$\exists t_0 \in]0,1[\quad \langle t_0 x_1 + (1 - t_0) w(x_2), \alpha \rangle = 0.$$

Première méthode : La FIG. 6.7 nous rappelle une démonstration du Théorème de régionnement du plan par la médiatrice d'un segment (voir leçon d'oral 1 du CAPES, [17], Chap. 3). On calque sur cette démonstration.
Si $x, y \in \mathbb{R}^n$, posons $d(x,y) = ||x - y||$. Les vecteurs x_1 et $s_\alpha(w(x_2))$ appartiennent au même demi-espace ouvert de frontière P_α, et z n'appartient pas au segment $[x_1; s_\alpha(w(x_2))]$ (sinon z appartiendrait au demi-espace ouvert de frontière P_α contenant x_1 par convexité des demi-espaces, impossible), donc

$$d(x_1, s_\alpha(w(x_2))) < d(x_1, z) + d(z, s_\alpha(w(x_2))).$$

Par symétrie $d(z, s_\alpha(w(x_2))) = d(z, w(x_2))$, donc

$$d(x_1, s_\alpha(w(x_2))) < d(x_1, z) + d(z, w(x_2)) = d(x_1, w(x_2)),$$

c'est-à-dire $||x_1 - s_\alpha(w(x_2))|| < ||x_1 - w(x_2)||$, ce qui est absurde.

Seconde méthode : Par définition, $s_\alpha(w(x_2)) = w(x_2) - N\alpha$, où l'on pose $N = 2\dfrac{\langle \alpha, w(x_2) \rangle}{||\alpha||^2}$. On a

$$\begin{aligned} ||x_1 - s_\alpha(w(x_2))||^2 &= \langle\, x_1 - w(x_2) + N\alpha, x_1 - w(x_2) + N\alpha \,\rangle \\ &= ||x_1 - w(x_2)||^2 + N^2||\alpha||^2 + 2\langle x_1 - w(x_2), N\alpha \rangle. \end{aligned}$$

D'où

$$\begin{aligned} ||x_1 - s_\alpha(w(x_2))||^2 &= ||x_1 - w(x_2)||^2 + 2N\langle x_1, \alpha \rangle \\ &= ||x_1 - w(x_2)||^2 + 4\frac{\langle \alpha, w(x_2) \rangle}{||\alpha||^2}\langle x_1, \alpha \rangle. \end{aligned}$$

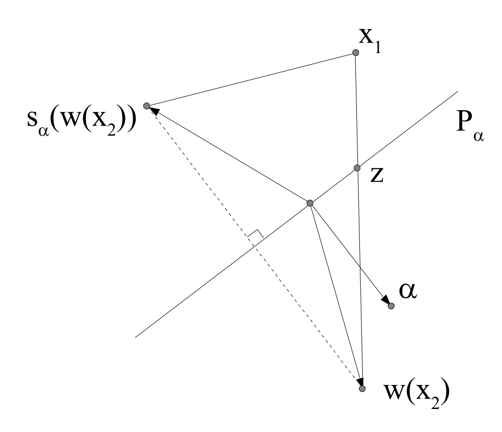


FIG. 6.7 – Régionnement de l'espace par P_α

Mais $\langle t_0x_1 + (1-t_0)w(x_2), \alpha\rangle = 0$ donne $(1-t_0)\langle w(x_2), \alpha\rangle = -t_0\langle x_1, \alpha\rangle$, donc

$$||x_1 - s_\alpha(w(x_2))||^2 = ||x_1 - w(x_2)||^2 - 4\frac{t_0}{(1-t_0)||\alpha||^2}\langle x_1, \alpha\rangle^2 .$$

Comme $t_0 \in]0,1[$, l'expression $4\frac{t_0}{(1-t_0)||\alpha||^2}\langle x_1, \alpha\rangle^2$ est strictement positive, et l'on obtient bien

$$||x_1 - s_\alpha(w(x_2))||^2 < ||x_1 - w(x_2)||^2,$$

ce qui contredit la définition de w.

VI.4.c. De $I \subset C_1$ on tire $w(x_2) \in C_1$. Comme w permute les chambres de Weyl (VI.3), $w(C_2)$ est un chambre de Weyl qui contient $w(x_2)$, donc qui intercepte C_1. Par suite $w(C_2) = C_1$. On a montré que

$$\forall C_1,\ C_2 \text{ chambres de Weyl} \qquad \exists w \in W \qquad w(C_2) = C_1,$$

et cela signifie que le groupe W opère transitivement sur les chambres de Weyl.

VI.5.a. • Montrer que $C(B) \subset \Omega$ revient à montrer que

$$\forall \alpha \in R \qquad C(B) \cap P_\alpha = \varnothing,$$

ou encore

$$\forall \alpha \in R^+ \qquad C(B) \cap P_\alpha = \varnothing, \quad (*)$$

puisque $P_\alpha = P_{-\alpha}$. Si $\alpha \in R^+$, III.1.b montre l'existence de n entiers naturels λ_1, ..., λ_n tels que $\alpha = \lambda_1\beta_1 + ... + \lambda_n\beta_n$, de sorte que

$$x \in C(B) \quad \Rightarrow \quad \langle x, \alpha\rangle = \sum_{i=1}^{n} \lambda_i \langle x, \beta_i\rangle > 0 \quad \Rightarrow \quad x \notin P_\alpha.$$

$(*)$ est bien démontrée.

• Montrons que $C(B)$ est convexe. Cela permettra d'affirmer que $C(B)$ est connexe par arcs, donc connexe, puis d'appliquer VI.2 : $C(B)$ étant connexe et inclus dans Ω, il existera une chambre de Weyl C telle que $C(B) \subset C$.
Soient donc $x, y \in C(B)$ et $t \in [0,1]$. Pour tout i,

$$\langle tx + (1-t)y, \beta_i\rangle = t\langle x, \beta_i\rangle + (1-t)\langle y, \beta_i\rangle > 0,$$

donc $tx+(1-t)y \in C(B)$ et l'intervalle $[x, y]$ est entièrement inclus dans $C(B)$. La partie $C(B)$ est bien connexe.

VI.5.b. C_i^+ est un ouvert comme l'intersection de l'ouvert C et du demi-plan ouvert $\{x \in \mathbb{R}^n \,/\, \langle x, \beta_i\rangle > 0\}$. De même, C_i^- est ouverte. On a $C_i^+ \cup C_i^- \subset C$, mais aussi $C \subset C_i^+ \cup C_i^-$ puisque tout élément x appartenant à C vérifie $\langle x, \beta_i\rangle \neq 0$. Ainsi $C_i^+ \cup C_i^- = C$.
Clairement $C_i^+ \cap C_i^- = \varnothing$ puisqu'un réel non nul $\langle x, \beta_i\rangle$ est soit positif, soit négatif, mais ne peut pas être les deux à la fois !
Comme C est connexe, C ne peut pas s'écrire comme la réunion de deux ouverts non vides, et l'un des deux ensembles C_i^+ ou C_i^- doit être vide.
En fait $C(B) \subset C_i^+$ et $C(B) \neq \varnothing$ (puisque $\beta_1' + ... + \beta_n' \in C(B)$), donc $C_i^- = \varnothing$ et $C = C_i^+$.

Remarque : Le demi-plan ouvert $\{x \in \mathbb{R}^n \,/\, \langle x, \beta_i\rangle > 0\}$ est ouvert comme l'image réciproque de l'ouvert $\mathbb{R}_+^*$ par l'application continue $x \mapsto \langle x, \beta_i\rangle$, cette dernière application étant continue comme toutes les applications linéaires dont l'ensemble de départ est un espace vectoriel de dimension finie.

VI.5.c. Puisque $C = C_i^+$ pour tout i, tout élément x de C vérifie $\langle x, \beta_i\rangle > 0$ pour tout i, donc appartient à $C(B)$. Ainsi $C \subset C(B)$. L'inclusion $C(B) \subset C$ ayant été démontrée en VI.5.a, on en déduit $C(B) = C$.

VI.6. Voir FIG. 6.8.

VI.7.a. Soient :

- $\preceq$ un ordre total compatible avec la structure vectorielle de $\mathbb{R}^n$,
- B une base du système de racines R associé à cet ordre. On a donc $B = (\beta_1, ..., \beta_n)$ où les β_i sont les racines simples de R (pour $\preceq$).

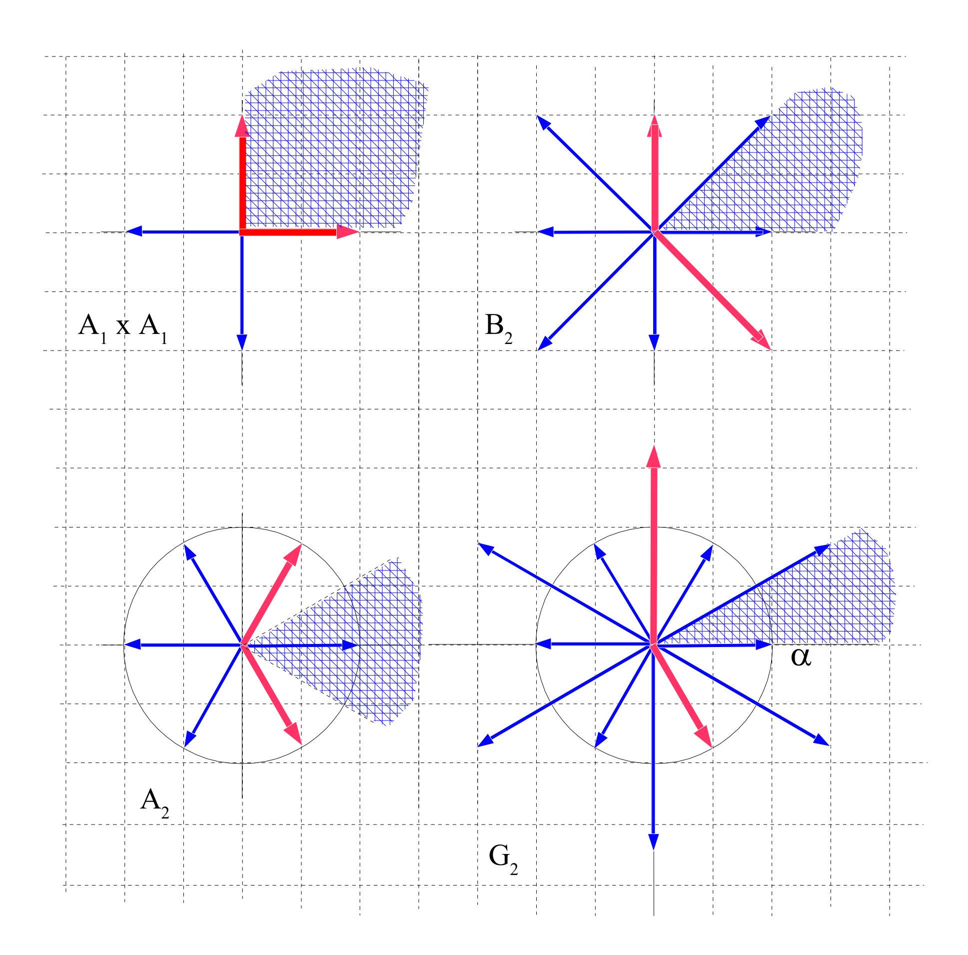


FIG. 6.8 – Chambres de Weyl fondamentales

Comme W opère transitivement sur les chambres de Weyl (VI.4.c), il existe $w \in W$ tel que $w(C(B)) = C$. Introduisons l'ordre $\preceq_w$ déduit de $\preceq$ en posant

$$x \preceq_w y \quad \Leftrightarrow \quad w^{-1}(x) \preceq w^{-1}(y)$$

(comme à la question II.1.b). On a

$$0 \prec_w w(\beta_i) \quad \Leftrightarrow \quad 0 \prec \beta_i,$$

donc les racines positives (pour $\preceq_w$ et $\preceq$) se correspondent. Mieux, comme w est linéaire bijective, si β est racine simple pour $\preceq$, alors $w(\beta)$ est racine simple pour $\preceq_w$. Cela montre que la famille $w(B) = (w(\beta_1), ..., w(\beta_n))$ est une base de R associée à l'ordre $\preceq_w$.

Enfin $w(C(B)) = C(w(B))$ puisque w conserve le produit scalaire (c'est une application orthogonale !). En effet :

$$\begin{aligned} x \in C(w(B)) &\Leftrightarrow \forall i \quad \langle x, w(\beta_i)\rangle > 0 \\ &\Leftrightarrow \forall i \quad \left\langle w^{-1}(x), \beta_i\right\rangle > 0 \\ &\Leftrightarrow w^{-1}(x) \in C(B) \\ &\Leftrightarrow x \in w(C(B)). \end{aligned}$$

On a trouvé une base $w(B)$ de R telle que $C = w(C(B)) = C(w(B))$.

VI.7.b. La question précédente montre que l'application

$$\Phi : \begin{array}{ccc} \text{Bases de } R & \to & \text{Chambres de } R \\ B & \mapsto & C(B) \end{array}$$

est surjective. Montrons qu'elle est injective. Soit C une chambre de R. Considérons deux bases $B = (\beta_1, ..., \beta_n)$ et $\widetilde{B} = (\widetilde{\beta}_1, ..., \widetilde{\beta}_n)$ de R telles que $C(B) = C(\widetilde{B}) = C$, et notons $(\beta_1', ..., \beta_n')$ et $(\widetilde{\beta}_1', ..., \widetilde{\beta}_n')$ leurs bases duales. On a

$$C = C(B) = \left\{ \sum_{i=1}^{n} x_i \beta_i' \,/\, x_1, ..., x_n \in \mathbb{R}_+^* \right\},$$

donc C est un cône de génératrices maximales les demi-droites $\mathbb{R}_+ \beta_i'$.
De la même façon,

$$C = C(\widetilde{B}) = \left\{ \sum_{i=1}^{n} x_i \widetilde{\beta}_i' \,/\, x_1, ..., x_n \in \mathbb{R}_+^* \right\},$$

donc C est un cône de génératrices maximales les demi-droites $\mathbb{R}_+ \beta_i'$.
Quitte à réindexer l'une des bases B ou $\widetilde{B}$, on peut affirmer que pour tout i, les vecteurs β_i' et $\widetilde{\beta}_i'$ sont colinéaires et de même sens (le fait de réindexer l'une des bases signifie que, dans la définition de l'ensemble de départ de Φ, on ne s'intéresse aux bases de R "qu'à permutation près de ses éléments"). On en déduit que pour tout i, β_i et $\widetilde{\beta}_i$ sont colinéaires et de même sens, donc égaux (puisqu'il s'agit de vecteurs appartenant au même système de racines R).
Finalement $B = \widetilde{B}$, et l'on a montré :

$$\Phi(B) = \Phi(\widetilde{B}) \quad \Rightarrow \quad B = \widetilde{B},$$

c'est-à-dire l'injectivité de Φ.

VI.8.a. Pour tout $i \in \{1, ..., p-1\}$ posons $\alpha_i = s_{\beta_i} \circ ... \circ s_{\beta_{p-1}}(\beta_p)$. Posons $\alpha_p = \beta_p$. Par hypothèse,

$$\begin{cases} \alpha_p = \beta_p \in R^+ \\ \alpha_1 = s_{\beta_1} \circ ... \circ s_{\beta_{p-1}}(\beta_p) \in R^-, \end{cases}$$

et l'on peut définir

$$q = \mathrm{Max}\left\{i \in \{1, ..., p-1\} \;/\; \alpha_i \in R^-\right\}.$$

On a $s_{\beta_q}(\alpha_{q+1}) = \alpha_q \in R^-$. Si l'on suppose $\beta_q \neq \alpha_{q+1}$, la question IV.3.b permet d'écrire

$$\left.\begin{array}{l} \beta_q \neq \alpha_{q+1} \\ \alpha_{q+1} \in R^+ \\ \beta_q \in B \end{array}\right\} \Rightarrow \quad s_{\beta_q}(\alpha_{q+1}) = \alpha_q \in R^+$$

d'où $\alpha_q \in R^- \cap R^+$, ce qui ne se peut pas. Donc

$$\beta_q = \alpha_{q+1} = s_{\beta_{q+1}} \circ ... \circ s_{\beta_{p-1}}(\beta_p).$$

L'application orthogonale $\varphi = s_{\beta_{q+1}} \circ ... \circ s_{\beta_{p-1}}$ comme toute composée de réflexions, et vérifie $\varphi(\beta_p) = s_{\beta_{q+1}} \circ ... \circ s_{\beta_{p-1}}(\beta_p) = \alpha_{q+1} = \beta_q$.
La question IV.1 donne alors :

$$s_{\beta_q} = s_{\varphi(\beta_p)} = \varphi \circ s_{\beta_p} \circ \varphi^{-1}.$$

Par suite

$$\begin{aligned} s_{\beta_1} \circ ... \circ s_{\beta_p} &= (s_{\beta_1} \circ ... \circ s_{\beta_{q-1}}) \circ s_{\beta_q} \circ (s_{\beta_{q+1}} \circ ... \circ s_{\beta_p}) \\ &= (s_{\beta_1} \circ ... \circ s_{\beta_{q-1}}) \circ \varphi \circ s_{\beta_p} \circ \varphi^{-1} \circ \left(\varphi \circ s_{\beta_p}\right) \\ &= (s_{\beta_1} \circ ... \circ s_{\beta_{q-1}}) \circ \varphi \\ &= s_{\beta_1} \circ ... \circ s_{\beta_{q-1}} \circ s_{\beta_{q+1}} \circ ... \circ s_{\beta_{p-1}}. \end{aligned}$$

Remarque : Pas de panique... le problème devient quasiment infaisable à partir de la question VI.5, donc aucun candidat ne traitera ces dernières questions en situation. Durant sa préparation, on se contentera tout au plus de lire la solution et de la comprendre.

VI.8.b. D'après IV.4.c, w peut s'écrire sous la forme

$$w = s_{\beta_1} \circ ... \circ s_{\beta_p}$$

avec β_1, ..., $\beta_p \in B$, et l'on peut supposer que le nombre de réflexions s_β employées dans cette expression est minimal. Alors

$$w(\beta_p) = s_{\beta_1} \circ ... \circ s_{\beta_p}(\beta_p) = -s_{\beta_1} \circ ... \circ s_{\beta_{p-1}}(\beta_p).$$

Si l'on avait $w(\beta_p) \in R^+$, VI.8.a montrerait l'existence de $q \in \{1, ..., p-1\}$ tel que

$$w = s_{\beta_1} \circ ... \circ s_{\beta_p} = s_{\beta_1} \circ ... \circ s_{\beta_{q-1}} \circ s_{\beta_{q+1}} \circ ... \circ s_{\beta_{p-1}},$$

et cette décomposition serait plus courte que celle dont on était parti ! C'est absurde, donc $w(\beta_p) \in R^-$.

VI.9.a. • *W opère transitivement sur les bases ?*

W opère transitivement sur les chambres de Weyl. Si B et B' sont deux bases de R, il existe donc $w \in W$ tel que $w(C(B)) = C(B')$. Dans la preuve de la question VI.7.a, on a montré que $w(C(B)) = C(w(B))$, donc

$$C(w(B)) = C(B').$$

En raisonnant sur des cônes comme en VI.7.a, on en déduit $w(B) = B'$ après permutation éventuelle des vecteurs de base.

• *W opère simplement sur les bases ?*

Il s'agit de montrer que l'élément $w \in W$ tel que $w(B) = B'$ est unique. Si $w' \in W$ vérifie $w'(B) = B'$, alors $w'^{-1} \circ w(B) = B$. Si l'on avait $w'^{-1} \circ w \neq Id$, VI.8.b montrerait l'existence de $\beta \in B$ tel que $w'^{-1} \circ w(\beta) \in R^-$, ce qui est absurde puisque $w'^{-1} \circ w(\beta) \in B \subset R^+$ et $R^- \cap R^+ = \varnothing$.
Par suite $w'^{-1} \circ w = Id$ et $w = w'$.

VI.9.b. D'après VI.4.c, W opère transitivement sur les chambres de Weyl. Pour montrer que cette action de groupe est simple, il s'agit de prouver que

$$w(C) = w'(C) \quad \Rightarrow \quad w = w',$$

autrement dit que

$$w(C) = C \quad \Rightarrow \quad w = Id,$$

où C désigne une chambre de Weyl donnée.
Soit B la base associée à C par la question VI.7a. On a $C = C(B)$, et en raisonnant comme dans la preuve de VI.7a,

$$C = w(C) = w(C(B)) = C(w(B)),$$

donc $C(B) = C(w(B))$. Cela entraîne $B = w(B)$ (toujours comme en VI.7a), puis $w = Id$ en appliquant VI.9.a.

Chapitre 7

CAPES externe 2008, épreuve 2

7.1 Énoncé

A propos d'un théorème de Tchebychev
sur la répartition des nombres premiers

Introduction

Etant donné un entier naturel n, on considère $\pi(n)$ le nombre de nombres premiers compris entre 0 et n. Ce sujet s'intéresse au comportement de la suite $(\pi(n))_n$. Il est composé de deux grandes parties A et B.

La partie A vise à établir l'encadrement suivant :

$$(\ln 2)\,\frac{n}{\ln n} \leq \pi(n) \leq e\frac{n}{\ln n}$$

valable pour tout $n \geq 3$. Elle est composée de deux sous-parties, A.I et A.II, consacrées respectivement à la minoration et à la majoration annoncées.

Ce genre d'encadrement suggère l'existence d'un lien asymptotique fort entre les suites $(\pi(n))_n$ et$(\frac{n}{\ln n})_n$. La partie B s'intéresse à cette question puisque son objectif principal est de montrer le résultat suivant :

Théorème.— (Tchebychev[1]) S'il existe un réel $c > 0$ telle que $\pi(n) \sim c\frac{n}{\ln n}$ alors nécessairement $c = 1$.

[1]Pafnouti Lvovitch Tchebychev, mathématicien russe, Okatovo 1821 - Saint-Pétersbourg 1894.

Elle est composée de quatre sous-parties B.I, B.II, B.III et B.IV. C'est dans la partie B.III qu'on établit le théorème annoncé. La preuve qu'on en propose repose sur l'étude du comportement asymptotique de la suite $\left(\sum_{p \text{ premier } \leq n} \frac{1}{p}\right)_n$. Cette étude est réalisée au début de la partie B.III. Les parties B.I et B.II sont consacrées à l'établissement de formules importantes pour la suite. Dans la partie B.I on établit une formule due à Legendre[2] qui donne l'expression de la valuation p-adique de $n!$. Dans la partie B.II on démontre un théorème de Mertens[3] qui précise le comportement asymptotique de la suite $\left(\sum_{p \text{ premier } \leq n} \frac{1}{p}\right)_n$. La partie B.IV est une application de la formule asymptotique trouvée dans la partie B.III. On y étudie la *densité* de l'ensemble des entiers possédant de *grands facteurs premiers.*

A la fin du sujet, une note documentaire met en perspective, d'un point de vue historique, le théorème de Tchebychev démontré ici. Sa lecture n'est pas essentielle au bon traitement du sujet.

Les parties de ce problème ne sont pas indépendantes entre elles.

Notations et rappels

• On note $\mathcal{P}$ l'ensemble des nombres premiers positifs.

• Si E désigne un ensemble fini, on note $\#E$ le cardinal de cet ensemble, c'est-à-dire le nombre d'éléments de E.

• Si $(u_n)_n$ et $(v_n)_n$ désignent deux suites numériques, on notera $u_n \sim v_n$ pour dire que ces suites sont équivalentes. On notera $u_n = o(v_n)$ pour dire que la suite $(u_n)_n$ est négligeable devant la suite $(v_n)_n$ et enfin, on notera $u_n = O(v_n)$ pour dire que la suite $(u_n)_n$ est dominée par la suite $(v_n)_n$, c'est-à-dire, qu'il existe un réel c et un entier n_0 tels que pour tout $n \geq n_0$ on ait $|u_n| \leq c\,|v_n|$.

• Si x désigne un réel, on notera $[x]$ sa partie entière, c'est-à-dire le plus grand entier inférieur ou égal à x ; autrement dit, $[x]$ est l'unique élément de $\mathbb{Z}$ vérifiant :

$$[x] \leq x < [x] + 1.$$

On rappelle que si a et b sont deux entiers tels que $0 \leq b \leq a$, le coefficient binomial $\binom{a}{b}$ est égal à $\frac{a!}{(a-b)!b!}$.

[2] Adrien-Marie Legendre, mathématicien français, Paris 1752 - Auteuil 1833.

[3] Franz Mertens, mathématicien autrichien, 1840 - 1927.

• Pour tout entier $n \geq 0$, on note $\pi(n)$ le nombre de nombres premiers compris dans l'intervalle $[0, n]$; ainsi on a $\pi(0) = \pi(1) = 0$, $\pi(2) = 1$, $\pi(3) = 2$, $\pi(4) = 2$, etc.
Pour tout entier $n \geq 1$, on note $\delta(n) = \pi(n) - \pi(n-1)$, de sorte que si l'on pose $\delta(0) = 0$, on voit que δ est la fonction caractéristique de $\mathcal{P}$ dans $\mathbb{N}$ (c'est-à-dire, $\delta(n)$ vaut 1 si n est premier, et 0 sinon).

• **Dans tout ce texte la lettre p désignera toujours et exclusivement un nombre premier**, ceci y compris lorsque la lettre p sera utilisée comme symbole d'indice d'une somme ou d'un produit. Par exemple, la notation $\sum_{p \leq x} \frac{1}{p}$ désigne la somme des inverses des nombres premiers p inférieurs ou égaux au réel x.

• Etant donnés un entier $n \geq 1$ et un nombre premier p, on appelle valuation p-adique de n l'entier noté $v_p(n)$ et égal à l'exposant de p dans la décomposition en facteurs premiers de n. Par exemple, si l'on prend $n = 350 = 2.5^2.7$ on a $v_2(350) = 1$, $v_3(350) = 0$, $v_5(350) = 2$, $v_7(350) = 1$ et $v_p(350) = 0$ pour tout nombre premier $p \geq 11$.

On admet les propriétés élémentaires suivantes :

a) $v_p(n)$ est l'entier k tel que p^k divise n et p^{k+1} ne divise pas n.

b) Pour tout $n \geq 1$ fixé, la suite $(v_p(n))_{p \in \mathcal{P}}$ est nulle à partir d'un certain rang, de sorte que l'on peut écrire $n = \prod_{p \in \mathcal{P}} p^{v_p(n)}$ (ce produit pouvant alors être considéré comme un produit fini). Cette écriture n'est alors rien d'autre que la décomposition en facteurs premiers de l'entier n.

c) Pour tous n, m entiers naturels non nuls et tout $p \in \mathcal{P}$, on a

$$v_p(nm) = v_p(n) + v_p(m).$$

Aucune preuve de ces trois résultats n'est demandée aux candidats.

Partie A : UNE ESTIMATION A LA TCHEBYCHEV

I. Une minoration de la fonction π

On considère, pour tout entier $n \geq 1$, l'entier $\Delta_n = \text{ppcm}(1, 2, ..., n)$. Dans cette partie nous allons établir une minoration de Δ_n. Nous en déduirons ensuite une minoration de $\pi(n)$. On considère $a, b \in \mathbb{N}$ vérifiant $1 \leq b \leq a$ et l'on pose :

$$I(b, a) = \int_0^1 x^{b-1} (1-x)^{a-b} \, dx.$$

A.I.1.

A.I.1.a. Expliciter $I(1,a)$ en fonction de a.

A.I.1.b. Montrer que si $b<a$ alors $I(b+1,a)=\dfrac{b}{a-b}I(b,a)$.

A.I.1.c. En déduire que $I(b,a)=\frac{1}{b\binom{a}{b}}$.

A.I.2. On se propose dans cette question de donner une autre méthode pour calculer $I(b,a)$. On considère un réel $y\in[0,1[$.

A.I.2.a. En développant à l'aide de la formule du binôme de Newton, montrer que :

$$\int_0^1 (1-x+xy)^{a-1}\,dx=\sum_{k=1}^{a}\binom{a-1}{k-1}y^{k-1}I(k,a).$$

A.I.2.b. En calculant maintenant directement l'intégrale, montrer que :

$$\int_0^1 (1-x+xy)^{a-1}\,dx=\frac{1}{a}\sum_{k=1}^{a}y^{k-1}.$$

A.I.2.c. En déduire que $I(b,a)=\frac{1}{b\binom{a}{b}}=\frac{1}{a\binom{a-1}{b-1}}$.

A.I.3.

A.I.3.a. Montrer que $I(b,a)=\displaystyle\sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\frac{1}{k+b}$.

A.I.3.b. En déduire que $I(b,a)\,\Delta_a\in\mathbb{N}$.

A.I.3.c. Prouver que l'entier $b\binom{a}{b}$ divise l'entier Δ_a.

A.I.4. Soit $n\geq 1$ un entier.

A.I.4.a. Montrer que les entiers $n\binom{2n}{n}$ et $(2n+1)\binom{2n}{n}$ divisent l'entier Δ_{2n+1}. (Indication : On remarquera que pour tout $k\geq 1$, Δ_k divise Δ_{k+1}.)

A.I.4.b. En déduire que l'entier $n(2n+1)\binom{2n}{n}$ divise Δ_{2n+1}. (Indication : On remarquera que les entiers n et $2n+1$ sont toujours premiers entre eux.)

A.I.4.c. Montrer que pour tout $k\in\{0,...,2n\}$ on a l'inégalité $\binom{2n}{k}\leq\binom{2n}{n}$.

A.I.4.d. En déduire que $(2n+1)\binom{2n}{n}\geq 4^n$. (Indication : On développera l'égalité $4^n=(1+1)^{2n}$.)

A.I.4.e. En déduire que $\Delta_{2n+1}\geq n4^n$.

A.I.4.f. Montrer que si $n\geq 9$ alors $\Delta_n\geq 2^n$ et vérifier que cette inégalité est encore vraie pour $n=7$ et 8.

A.I.5. Soit $n\geq 1$ un entier.

A.I.5.a. Soit $p\in\mathcal{P}$, montrer que $p^{v_p(\Delta_n)}\leq n$. (Indication : On commencera par exprimer $v_p(\Delta_n)$ en fonction des entiers $v_p(1)$, ..., $v_p(n)$.)

A.I.5.b. Montrer que $\Delta_n = \prod_{p \leq n} p^{v_p(\Delta_n)}$.

A.I.5.c. En déduire que $\Delta_n \leq n^{\pi(n)}$.

A.I.6.

A.I.6.a. Montrer que pour tout $n \geq 7$ on a

$$\pi(n) \geq (\ln 2) \frac{n}{\ln n}.$$

A.I.6.b. Pour quels entiers $n \in \{2, 3, 4, 5, 6\}$ l'inégalité de la question précédente est-elle encore vraie ?

II. Une majoration de la fonction π

A.II.1. On cherche dans cette question à majorer simplement le produit $\prod_{p \leq n} p$ en fonction de l'entier $n \geq 1$.

A.II.1.a. Soient a et b deux entiers tels que $0 < \frac{b}{2} \leq a < b$. Montrer que le produit $\prod_{a < p \leq b} p$ divise l'entier $\binom{b}{a}$ (le produit considéré est supposé être égal à 1 dans le cas où il n'y aurait pas de nombre premier p dans l'intervalle $]a, b]$).

A.II.1.b. En déduire que pour tout $m \geq 1$, le produit $\prod_{m+1 < p \leq 2m+1} p$ divise l'entier $\binom{2m+1}{m+1}$.

A.II.1.c. Comparer, pour $m \geq 1$, les entiers $\binom{2m+1}{m}$ et $\binom{2m+1}{m+1}$.

A.II.1.d. En déduire que pour tout entier $m \geq 1$ on a $\binom{2m+1}{m} \leq 4^m$. (Indication : On développera la quantité $(1+1)^{2m+1}$.)

A.II.1.e. Montrer que pour tout entier $m \geq 1$, on a $\prod_{m+1 < p \leq 2m+1} p \leq 4^m$.

A.II.1.f. Prouver finalement que pour tout entier $n \geq 1$, on a

$$\prod_{p \leq n} p \leq 4^n.$$

(Indication : On pourra montrer par récurrence, pour $n \geq 1$, la propriété P_n : pour tout $k \in \{1, ..., 2n\}$ on a $\prod_{p \leq k} p \leq 4^k$.)

A.II.2.

A.II.2.a. Montrer que pour tout entier $m \geq 1$ on a $m! > \left(\frac{m}{e}\right)^m$. (Indication : On pourra penser au développement en série entière de la fonction exponentielle.)

A.II.2.b. Déduire de ce qui précède que, pour tout $n \geq 2$, on a $\pi(n)! \leq 4^n$ et que par suite, on a

$$\pi(n) \ln \pi(n) - \pi(n) \leq n \ln 4.$$

A.II.3. On souhaite montrer, à partir du résultat précédent, que pour tout $n \geq 3$ on a

$$\pi(n) \leq e\frac{n}{\ln n}.$$

Pour cela on raisonne par l'absurde, en supposant qu'il existe un entier $n_0 \geq 3$ tel que $\pi(n_0) > e\frac{n_0}{\ln n_0}$.

A.II.3.a. Montrer que la fonction $x \mapsto x \ln x - x$ est strictement croissante sur $[1, +\infty[$. En déduire que

$$\frac{e - \ln 4}{e} < \frac{\ln \ln n_0}{\ln n_0}.$$

A.II.3.b. Montrer que la fonction $x \mapsto \frac{\ln x}{x}$ est majorée par e^{-1} sur $[1, +\infty[$. Conclure.

Partie B : AUTOUR D'UN THEOREME DE MERTENS

I. Une formule de Legendre sur la valuation p-adique de $n!$

On considère un entier $n \geq 2$ et un nombre premier p. Pour tout entier $k \geq 0$, on considère les sous-ensembles finis U_k, V_k et Ω_k de $\mathbb{N}$ définis par

$$\begin{aligned} U_k &= \{a \in \{1, ..., n\} / p^k \text{ divise } a\}, \\ V_k &= \{a \in \{1, ..., n\} / p^k \text{ ne divise pas } a\}, \\ \Omega_k &= \{a \in \{1, ..., n\} / v_p(a) = k\}. \end{aligned}$$

B.I.1. Justifier qu'il existe un plus petit entier $k_0 \geq 0$ tel que $n < p^{k_0}$. Montrer que $k_0 \geq 1$ et expliciter k_0 en fonction de n et p.

B.I.2.

B.I.2.a. Montrer que, pour tout $k \in \{0, ..., k_0 - 1\}$, l'ensemble U_{k+1} est strictement inclus dans U_k et que pour $k \geq k_0$ on a $U_k = \varnothing$.

B.I.2.b. Montrer que, pour tout $k \in \{0, ..., k_0 - 1\}$, l'ensemble V_k est strictement inclus dans V_{k+1} et que pour $k \geq k_0$ on a $V_k = \{1, ..., n\}$.

B.I.2.c. Prouver que la famille de parties $\{\Omega_0, ..., \Omega_{k_0-1}\}$ forme une partition de l'ensemble $\{1, ..., n\}$.

B.I.3.

B.I.3.a. Pour tout $k \geq 0$, établir que $\Omega_k = U_k \cap V_{k+1}$.

B.I.3.b. Calculer, pour tout $k \geq 0$, $\#U_k$ et $\#V_k$ puis $\#\Omega_k$ en fonction de n, p.

B.I.4. Montrer que $v_p(n!) = \sum_{k\geq 0} k \,\#\Omega_k$ et en déduire que

$$v_p(n!) = \sum_{k\geq 1} \left[\frac{n}{p^k}\right]$$

(formule de Legendre).

II. Un théorème de Mertens

Dans toute cette partie II, on considère un entier $n \geq 2$.

B.II.1. Prouver que pour tout $p \in \mathcal{P}$ on a

$$\frac{n}{p} - 1 < v_p(n!) \leq \frac{n}{p} + \frac{n}{p(p-1)}$$

(Indication : On pourra utiliser l'encadrement $x - 1 < [x] \leq x$ valable pour tout réel x et la formule de Legendre.)

B.II.2. En déduire que

$$n\sum_{p\leq n} \frac{\ln p}{p} - \sum_{p\leq n} \ln p < \ln n! \leq n\sum_{p\leq n} \frac{\ln p}{p} + n\sum_{p\leq n} \frac{\ln p}{p(p-1)}.$$

(Indication : On pourra commencer par montrer que $n! = \prod_{p\leq n} p^{v_p(n!)}$.)

B.II.3. Dans cette question on établit plusieurs majorations techniques utiles aux deux questions suivantes.

B.II.3.a. Montrer la convergence de la série $\sum \frac{r}{2^r}$ et que $\sum_{r=1}^{+\infty} \frac{r}{2^r} = 2$. (Indication : On pourra s'intéresser à la série entière $\sum_{k\geq 0} \frac{x^k}{2^k}$ ainsi qu'à sa série dérivée.)

B.II.3.b. Calculer pour tout entier $r \geq 1$ la somme finie

$$\sum_{2^{r-1}<m\leq 2^r} \frac{1}{m(m-1)}.$$

En déduire que si l'on pose $U_r = \sum_{2^{r-1}<m\leq 2^r} \frac{\ln m}{m(m-1)}$ alors on a $U_r \leq \frac{r}{2^r}\ln 2$.

B.II.3.c. Montrer que la série $\sum U_r$ converge. Donner un majorant de $\sum_{r=1}^{+\infty} U_r$.

B.II.3.d. En déduire que la série $\sum \frac{\ln m}{m(m-1)}$ est convergente et que l'on a :

$$\sum_{m=2}^{+\infty} \frac{\ln m}{m(m-1)} \leq \ln 4.$$

B.II.3.e. Montrer que $1 - \frac{1}{2n} \leq n\ln(1+\frac{1}{n}) \leq 1$ et $\ln(1+\frac{1}{n}) \geq \frac{1}{2n}$. (Indication : On commencera par déterminer pour quels réels u on a les inégalités $u - u^2/2 \leq \ln(1+u) \leq u$.)

B.II.3.f. En déduire, par récurrence sur n, qu'il existe un réel $\theta_n \in [0,1]$ tel que : $\ln n! = n\ln n - n + 1 + \theta_n \ln n$.

B.II.4. Prouver, en utilisant les résultats des questions B.II.2 et B.II.3, que :

$$\ln n - (1+\ln 4) \leq \sum_{p\leq n} \frac{\ln p}{p}.$$

B.II.5. De même, en utilisant les questions B.II.2, B.II.3 et A.II.1.f, montrer que :

$$\sum_{p\leq n} \frac{\ln p}{p} \leq \ln n + \ln 4.$$

En déduire que $\displaystyle\sum_{p\leq n} \frac{\ln p}{p} = \ln n + O(1)$ (théorème de Mertens).

III. Le comportement asymptotique de $\left(\sum_{p\leq n} \frac{1}{p}\right)_n$

B.III.1. Dans cette question on établit des résultats préliminaires utiles pour la suite.

B.III.1.a. Montrer que la série $\sum \frac{1}{n\ln^2 n}$ est convergente, que la série $\sum \frac{1}{n\ln n}$ est divergente et qu'on a

$$\sum_{k=2}^{n-1} \frac{1}{k\ln k} = \ln\ln n + O(1).$$

(Indication : On comparera les séries considérées avec les intégrales généralisées $\int_2^{+\infty} \frac{dt}{t\ln^2 t}$ et $\int_2^{+\infty} \frac{dt}{t\ln t}$.)

B.III.1.b. On considère la suite $(u_n)_{n\geq 3}$ définie par

$$u_n = \sum_{k=2}^{n-1} \frac{1}{k\ln k} - \ln\ln n.$$

Montrer que $u_{n+1} - u_n = \dfrac{1}{2n^2\ln n} + o\left(\dfrac{1}{n^2\ln n}\right)$.

B.III.1.c. En déduire qu'il existe un réel l tel que

$$\sum_{k=2}^{n-1} \frac{1}{k \ln k} = \ln \ln n + l + o(1).$$

B.III.2. On note $(\psi(n))_{n \geq 2}$ la suite définie par $\psi(n) = \sum_{p \leq n} \frac{\ln p}{p}$. On considère un entier $n \geq 3$.

B.III.2.a. Montrer que

$$\sum_{p \leq n} \frac{1}{p} = \sum_{k=2}^{n-1} \psi(k) \frac{\ln(1+1/k)}{\ln k \ln(k+1)} + \frac{\psi(n)}{\ln n}.$$

(Indication : On pourra remarquer que $\sum_{p \leq n} \frac{1}{p} = \sum_{k=2}^{n} \frac{\delta(k) \ln k}{k} . \frac{1}{\ln k}$ où δ est la fonction caractéristique de $\mathcal{P}$, puis utiliser la transformation d'Abel sous la forme suivante : si $(a_n)_{n \geq 1}$, $(b_n)_{n \geq 1}$ sont deux suites numériques et si pour $n \geq 1$ on pose $A_n = \sum_{k=1}^{n} a_k$, alors pour tout $N \geq 2$, on a

$$\sum_{n=1}^{N} a_n b_n = A_N b_N + \sum_{n=1}^{N-1} A_n (b_n - b_{n+1}).)$$

B.III.2.b. Prouver, en utilisant le théorème de Mertens, que :

$$\psi(k) \frac{\ln(1+1/k)}{\ln k \ln(k+1)} = \frac{1}{k \ln k} + O\left(\frac{1}{k \ln^2 k}\right).$$

(Indication : On commencera par écrire la fraction $\frac{\ln(1+1/k)}{\ln k \ln(k+1)}$ sous la forme $\frac{1}{\ln k} \frac{t(k)}{1+t(k)}$, où $t(k)$ est une suite qu'on déterminera. On montrera ensuite que $\frac{t(k)}{1+t(k)} = \dfrac{1}{k \ln k} - \dfrac{1}{2k^2 \ln k} + o(\dfrac{1}{k^2 \ln k})$.)

B.III.3. Déduire de ce qui précède qu'il existe une constante $\lambda \in \mathbb{R}$ telle que

$$\sum_{p \leq n} \frac{1}{p} = \ln \ln n + \lambda + o(1).$$

B.III.4. Montrer que pour tout $n \geq 2$ on a $\sum_{p \leq n} \frac{1}{p} = \sum_{k=2}^{n-1} \frac{\pi(k)}{k(k+1)} + \frac{\pi(n)}{n}$. En déduire que s'il existe une constante réelle c telle que $\pi(n) \sim c \frac{n}{\ln n}$ alors $c = 1$ (théorème de Tchebychev).

IV. Une application à l'étude des entiers possédant de grands facteurs premiers

Etant donné un entier $n \geq 2$, on note $P^+(n)$ le plus grand facteur premier apparaissant dans la décomposition en facteurs premiers de n. Par exemple, $P^+(50) = P^+(2.5^2) = 5$. On s'intéresse dans cette question à l'ensemble A constitué des entiers $n \geq 2$ vérifiant $P^+(n) > \sqrt{n}$ (c'est ce qu'on entend par *entiers possédant de grands facteurs premiers* dans le titre de cette partie). L'objectif de cette partie est de montrer que l'ensemble A possède une densité valant $\ln 2$. En d'autres termes, si pour un réel $x \geq 2$ on pose $A\,(x) = A \cap [0, x]$ et $a(x) = \#A(x)$ le cardinal de $A(x)$, nous allons montrer que la suite $(\frac{a(n)}{n})_n$ possède une limite (on dira alors que A possède une densité) et que cette limite vaut $\ln 2$ (qui sera donc appelée la densité de A). Ce résultat signifiera que, « moralement », il y a une proportion de $\ln 2 \simeq 0,69$ d'entiers dans $\mathbb{N}$ qui possèdent de grands facteurs premiers.

B.IV.1. En utilisant la question B.III.3 montrer que la suite $\left(\sum_{\sqrt{n} \leq p \leq n} \frac{1}{p}\right)_n$ possède une limite et donner cette limite.

B.IV.2. Soit $x \geq 2$ un réel.

B.IV.2.a. Soient $p \in \mathcal{P}$, $m \in \mathbb{N}^*$ et $n = mp$. Montrer que

$$\big(p = P^+\,(n) \text{ et } n \in A\,(x)\big) \quad \Leftrightarrow \quad m < p \leq x/m.$$

B.IV.2.b. Soient $p, p' \in \mathcal{P}$ et $m, m' \in \mathbb{N}^*$ tels que $m < p \leq x/m$ et $m' < p \leq x/m'$. Montrer que

$$mp = m'p' \quad \Leftrightarrow \quad \big(p = p' \text{ et } m = m'\big)\,.$$

B.IV.2.c. En déduire que les entiers de la forme mp avec $p \in \mathcal{P}$, $m \in \mathbb{N}^*$, et vérifiant $m < p \leq x/m$ décrivent de manière biunivoque l'ensemble $A(x)$.

B.IV.2.d. Prouver finalement que

$$a\,(x) = \sum_{p \leq x} \text{Min}\left(p - 1, \left[\frac{x}{p}\right]\right).$$

B.IV.3. Soit $x \geq 1$ un réel.

B.IV.3.a. Montrer que pour tout nombre premier p, on a l'équivalence

$$p - 1 \leq [x/p] \quad \Leftrightarrow \quad p \leq \varphi\,(x)$$

où $\varphi\,(x) = \dfrac{1 + \sqrt{1 + 4x}}{2}$.

B.IV.3.b. Montrer que $\sqrt{x} < \varphi(x) < \sqrt{x} + 1$.

B.IV.3.c. En déduire que $a(x) = \sum_{p \leq \sqrt{x}} (p-1) + \sum_{\sqrt{x} < p \leq x} [x/p]$.

(Indication : On examinera le cas où il existe un nombre premier dans l'intervalle $]\sqrt{x}, \varphi(x)]$ et le cas où il n'en existe pas.)

B.IV.3.d. En utilisant les encadrements obtenus dans la partie A, démontrer que $\sum_{p \leq \sqrt{x}} (p-1) = o(x)$.

B.IV.3.e. En utilisant la question B.IV.1 et les encadrements obtenus dans la partie A, montrer que $\sum_{\sqrt{x} < p \leq x} \left[\frac{x}{p}\right] = x \ln 2 + o(x)$.

B.IV.3.f. En déduire que $a(x) = x \ln 2 + o(x)$ et conclure.

FIN DE L'EPREUVE

Un peu d'histoire...

La notion de nombre premier est fondamentale en arithmétique des entiers. Très tôt dans l'histoire de l'esprit humain, en fait dès l'antiquité, on s'est intéressé à ces nombres.

On savait depuis cette époque qu'ils étaient en nombre infini (théorème d'Euclide[4]). Au cours des âges on s'est intéressé en particulier à leur mystérieuse répartition. Il faudra réellement attendre le XIXe siècle pour qu'on dispose d'idées et d'outils suffisamment sophistiqués pour mieux comprendre cette problématique.

Une première série d'idées importantes sur le sujet fut introduite par Tchebychev. En 1845 Bertrand[5] conjectura que pour tout entier $n \geq 2$ il existait toujours un nombre premier compris strictement entre n et $2n$. Il vérifia sa conjecture jusqu'au rang $n = 3\,000\,000$, mais il appartient à Tchebychev de la démontrer en 1851. Pour ce faire il entreprit de trouver des encadrements (qu'on appelle maintenant encadrements à la Tchebychev) de la fonction $\pi(n)$. Ces encadrements sont de la forme

$$\alpha \frac{n}{\ln n} \leq \pi(n) \leq \beta \frac{n}{\ln n}$$

pour $n \geq n_0$ effectif. L'objectif était de trouver des constantes α, β les plus proches possibles de 1 pour pouvoir conclure. Il y arrivera en montrant que cette inégalité est vraie pour $\alpha \simeq 0,92$ et $\beta \simeq 1,1$.

[4] Euclide, mathématicien probablement d'origine grecque, 330 av. J.-C. - 275 av. J.-C.

[5] Joseph Louis François Bertrand, mathématicien français, Paris 1822 - Paris 1900.

Dans la partie A de ce sujet nous établissons un tel encadrement mais avec des constantes ($\alpha \simeq 0,69$ et $\beta \simeq 2,72$) trop éloignées de 1 pour pouvoir conclure sur la conjecture de Bertrand. Ceci est dû aux méthodes d'encadrement utilisées.

A ce sujet, signalons que la méthode de minoration de $\pi(n)$ proposée en A.I repose sur la minoration effective de $\mathrm{ppcm}\,(1,...,n)$ par 2^n. Cette méthode de minoration de $\mathrm{ppcm}\,(1,...,n)$ est récente puisqu'elle date de 1982, elle est due à Nair. La majoration de $\pi(n)$ proposée en A.II repose sur la majoration effective de $\prod_{p\leq n} p$ par 4^n. Cette méthode de majoration de $\prod_{p\leq n} p$ est due à Erdos[6] et date de 1939.

Les encadrements à la Tchebychev laissent suggérer l'existence d'un lien étroit, en termes de comportement asymptotique, entre $\pi(n)$ et $\frac{n}{\ln n}$. En fait, il avait longtemps été conjecturé, notamment par Gauß[7] et Legendre, que l'on avait l'équivalence (théorème des nombres premiers) : $\pi\,(n) \sim \frac{n}{\ln n}$.

Il appartiendra à Hadamard[8] et de la Vallée-Poussin[9] de montrer (de manières indépendantes) ce résultat en 1896, confirmant ainsi la conjecture. Leur approche du problème fut la même et utilise l'analyse complexe. Elle repose sur l'étude sur la droite de partie réelle 1 de la fonction ζ de Riemann[10]. Pendant plusieurs années les experts, en particulier Hardy[11], ont pensé qu'une preuve du théorème des nombres premiers ne pouvait se dispenser de l'analyse complexe, tant il semblait que ce théorème était intrinsèquement lié aux propriétés de la fonction ζ. Pourtant en 1949 Erdos et Selberg[12] en proposèrent une preuve élémentaire (c'est-à-dire, n'utilisant pas d'analyse complexe). Daboussi a proposé en 1984 une nouvelle preuve élémentaire de ce théorème. Les considérations utilisées dans ces preuves élémentaires sont du même acabit que celles présentées dans ce sujet (en plus sophistiquées bien sûr, vu l'ampleur du résultat démontré).

On peut considérer que le théorème de Tchebychev dont il est question dans ce sujet fut historiquement l'une des premières avancées significatives vers le théorème des nombres premiers.

---

[6] Pál Erdos, mathématicien hongrois, Budapest 1913 - Varsovie 1996.

[7] Carl Friedrich Gauß, mathématicien allemand, Brunswick 1777 - Göttingen 1855.

[8] Jacques Salomon Hadamard, mathématicien français, Paris 1865 - Auteuil 1963.

[9] Charles Jean de La Vallée-Poussin, mathématicien belge, Louvain 1866 - Boitsfort 1962.

[10] Georg Friedrich Bernhard Riemann, mathématicien allemand, Breselenz 1826 - Selasca 1866.

[11] Godfrey Harold Hardy, mathématicien anglais, Cranleigh 1877 - Cambridge 1947.

[12] Atle Selberg, mathématicien norvégien, Langesund 1917.

7.2 Corrigé

Partie A : UNE ESTIMATION A LA TCHEBYCHEV

I. Une minoration de la fonction π

A.I.1.a. On a

$$I(1,a) = \int_0^1 (1-x)^{a-1}\ dx = \left[-\frac{(1-x)^a}{a}\right]_0^1 = \frac{1}{a}.$$

A.I.1.b. L'intégrant étant un produit de deux fonctions C^1 (en fait C^∞) sur $[0,1]$, on peut intégrer par parties :

$$\begin{aligned} I(b+1,a) &= \int_0^1 x^b (1-x)^{a-b-1}\ dx \\ &= \left[x^b \frac{-(1-x)^{a-b}}{a-b}\right]_0^1 - \int_0^1 bx^{b-1} \frac{-(1-x)^{a-b}}{a-b}\ dx \\ &= \frac{b}{a-b}\int_0^1 x^{b-1}(1-x)^{a-b}\ dx \\ &= \frac{b}{a-b} I(b,a). \end{aligned}$$

A.I.1.c. On utilise la formule de la question précédente autant de fois que nécessaire pour obtenir :

$$\begin{aligned} I(b,a) &= \frac{b-1}{a-b+1} I(b-1,a) \\ &= \frac{b-1}{a-b+1} \times \frac{b-2}{a-b+2} \times \ldots \times \frac{1}{a-1} I(1,a) \\ &= \frac{(b-1)!}{a(a-1)\ldots(a-b+1)} = \frac{1}{b\binom{a}{b}} \end{aligned}$$

puisque $\displaystyle\binom{a}{b} = \frac{a(a-1)\ldots(a-b+1)}{b!}$.

A.I.2.a. On a

$$\int_0^1 (1-x+xy)^{a-1}\ dx = \int_0^1 \sum_{i=0}^{a-1} \binom{a-1}{i} (1-x)^{a-1-i} (xy)^i\ dx.$$

En faisant le changement d'indice $i = k - 1$, on trouve

$$\begin{aligned}\int_0^1 (1-x+xy)^{a-1}\,dx &= \sum_{k=1}^{a} \binom{a-1}{k-1} y^{k-1} \int_0^1 x^{k-1}(1-x)^{a-k}\,dx \\ &= \sum_{k=1}^{a} \binom{a-1}{k-1} y^{k-1} I(k,a)\,.\end{aligned}$$

A.I.2.b. Un calcul direct donne

$$\begin{aligned}\int_0^1 (1-x+xy)^{a-1}\,dx &= \int_0^1 (1+(y-1)x)^{a-1}\,dx \\ &= \left[\frac{1}{y-1}\frac{(1+(y-1)x)^a}{a}\right]_0^1 \\ &= \frac{1}{a}\times\frac{y^a-1}{y-1}.\end{aligned}$$

Comme

$$\frac{y^a-1}{y-1} = 1+y+...+y^{a-1} = \sum_{k=1}^{a} y^{k-1},$$

on obtient bien la formule annoncée.

A.I.2.c. Les deux questions précédentes montrent que

$$\forall y \in [0,1[\quad \sum_{k=1}^{a}\binom{a-1}{k-1} I(k,a)\, y^{k-1} = \sum_{k=1}^{a}\frac{1}{a} y^{k-1}.$$

Pour a fixé, le polynôme à coefficients réels $\sum_{k=1}^{a}\left(\binom{a-1}{k-1} I(k,a) - \frac{1}{a}\right) Y^{k-1}$ admet une infinité de racines (tous les y appartenant à $[0,1[$), donc est égal au polynôme nul. Ainsi

$$\forall k \in \{1,...,a\}\quad \binom{a-1}{k-1} I(k,a) = \frac{1}{a}$$

soit

$$\forall b \in \{1,...,a\}\quad I(b,a) = \frac{1}{a\binom{a-1}{b-1}}.$$

Comme $a\binom{a-1}{b-1} = a\frac{(a-1)!}{(b-1)!\,(a-b)!} = b\frac{a!}{b!\,(a-b)!} = b\binom{a}{b}$, on obtient bien :

$$I(b,a) = \frac{1}{a\binom{a-1}{b-1}} = \frac{1}{b\binom{a}{b}}. \quad (1)$$

A.I.3.a.

$$I(b,a) = \int_0^1 x^{b-1}(1-x)^{a-b}\,dx = \int_0^1 x^{b-1}\sum_{k=0}^{a-b}\binom{a-b}{k}(-x)^k\,dx$$
$$= \sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\int_0^1 x^{k+b-1}\,dx.$$

Comme $\int_0^1 x^{k+b-1}\,dx = \left[\frac{x^{k+b}}{k+b}\right]_0^1 = \frac{1}{k+b}$, on obtient bien

$$I(b,a) = \sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\frac{1}{k+b}. \quad (2)$$

A.I.3.b. Quel que soit $k \in \{0,...,a-1\}$, $\binom{a-b}{k}$ est entier. La formule (2) exprime donc $I(b,a)$ comme une somme de fractions de dénominateurs b, $1+b$, $2+b$, ..., a. Par hypothèse, Δ_a est multiple de chacun de ces dénominateurs, donc il existe des entiers ξ_k tels que $\Delta_a = (k+b)\,\xi_k$ pour tous $k \in \{0,...,a-1\}$. L'égalité (2) entraîne alors

$$I(b,a)\,\Delta_a = \sum_{k=0}^{a-b}(-1)^k\binom{a-b}{k}\xi_k \in \mathbb{Z}$$

(somme de produits d'entiers).
Il suffit de rappeler que $I(b,a) = \int_0^1 x^{b-1}(1-x)^{a-b}\,dx$ est positif comme intégrale d'une fonction positive sur son intervalle de définition, pour conclure à $I(b,a)\,\Delta_a \in \mathbb{N}$.

A.I.3.c. En utilisant (1) et la question précédente, on obtient

$$I(b,a)\,\Delta_a = \frac{\Delta_a}{b\binom{a}{b}} \in \mathbb{N}$$

donc $b\binom{a}{b}$ divise Δ_a.

A.I.4.a. Pour tout k, Δ_{k+1} est un multiple de 1, 2, ..., $k+1$, donc a fortiori un multiple de 1, 2, ..., k, et à ce titre sera un multiple du ppcm Δ_k de 1, 2, ..., k. Donc :

$$\forall k \geq 1 \quad \Delta_k \text{ divise } \Delta_{k+1}.$$

Notons | la relation "divise". Les questions précédentes montrent que l'entier $b\binom{a}{b} = a\binom{a-1}{b-1}$ divise Δ_a.

• En prenant $a = 2n$ et $b = n$, on obtient

$$b\binom{a}{b} = n\binom{2n}{n} \mid \Delta_{2n} \mid \Delta_{2n+1}, \quad \text{donc } n\binom{2n}{n} \mid \Delta_{2n+1}.$$

• En prenant $a = 2n+1$ et $b = n+1$, je trouve

$$a\binom{a-1}{b-1} = (2n+1)\binom{2n}{n} \mid \Delta_{2n+1}.$$

A.I.4.b. Posons $c = \binom{2n}{n}$. D'après la question précédente, $nc \mid \Delta_{2n+1}$ et $(2n+1)\,c \mid \Delta_{2n+1}$. Il existe donc $q \in \mathbb{N}$ tel que

$$\Delta_{2n+1} = ncq.$$

Comme $(2n+1)\,c \mid ncq$, on en déduit $(2n+1) \mid nq$ d'où $(2n+1) \mid q$ en appliquant le Théorème de Gauss. Il existe donc $r \in \mathbb{N}$ tel que $q = r\,(2n+1)$, et en remplaçant,

$$\Delta_{2n+1} = n\,(2n+1)\,cr.$$

Cela prouve que $n\,(2n+1)\,c$ divise Δ_{2n+1}..

Remarques : α) Pour vérifier que n et $2n+1$ sont premiers entre eux, il suffit de prendre un diviseur d commun à ces deux nombres, puis de s'apercevoir qu'il divisera $2n+1-2\times n = 1$, donc que $d = \pm 1$. Le pgcd de n et $2n+1$ est donc 1.

β) L'utilisation que nous avons faite du Théorème de Gauss ([18], Co. 2) est un classique que l'on rencontre dans le cours, au moment où on démontre que, si a et b sont premiers entre eux et divisent le même nombre c, alors ab divise c. Si le lecteur sent qu'il doit réviser les faits basiques concernant la divisibilité dans $\mathbb{Z}$, il peut tout de suite lire la leçon d'oral concernant le pgcd de deux entiers et les nombres premiers entre eux ([18], Chap. 1). Cette leçon d'oral est à travailler consciencieusement pour les écrits et pour les oraux des concours !

A.I.4.c. On a

$$\binom{2n}{k} \le \binom{2n}{n} \;\Leftrightarrow\; \frac{(2n)!}{k!\,(2n-k)!} \le \frac{(2n)!}{n!\,n!} \;\Leftrightarrow\; (n!)^2 \le k!\,(2n-k)!.$$

• Si $k \le n$, alors $n \le 2n-k$ et la dernière inégalité écrite équivaut successivement à

$$\frac{n!}{k!} \le \frac{(2n-k)!}{n!}$$

$$n\,(n-1)\ldots(n-k+1) \leq (2n-k)(2n-k-1)\ldots(n-k+1)$$
$$1 \leq (2n-k)(2n-k-1)\ldots(n+1).$$

Cette dernière inégalité est triviale car un produit de nombres entiers naturels non nuls est toujours supérieur à 1. Donc $\binom{2n}{k} \leq \binom{2n}{n}$ dès que $k \leq n$.

• Si $k > n$, alors $n > 2n-k$ et on peut appliquer le point précédent pour obtenir :

$$\binom{2n}{k} = \binom{2n}{2n-k} \leq \binom{2n}{n}.$$

A.I.4.d. En utilisant la formule du binôme, on déduit

$$4^n = (1+1)^{2n} = \sum_{k=0}^{2n} \binom{2n}{k} \leq (2n+1)\binom{2n}{n}.$$

A.I.4.e. D'après A.1.4.b, $n\,(2n+1)\binom{2n}{n}$ divise Δ_{2n+1}, donc est inférieur à Δ_{2n+1}. En utilisant aussi la question précédente :

$$n4^n \leq n\,(2n+1)\binom{2n}{n} \leq \Delta_{2n+1}.$$

A.I.4.f. • Si n est impair, posons $n = 2m+1$. On a

$$\Delta_n = \Delta_{2m+1} \geq m4^m = m2^{2m} \geq 2^{2m+1}.$$

dès que $m \geq 2$, autrement dit dès que $n \geq 5$.

• Si n est pair, posons $n = 2m+2$. On a

$$\Delta_n = \Delta_{2m+2} \geq \Delta_{2m+1} \geq m4^m = m2^{2m} \geq 2^{2m+2}$$

dès que $m \geq 4$, autrement dit dès que $n \geq 10$.

On peut donc dire que $\Delta_n \geq 2^n$ pour tout $n \geq 9$. On vérifie que l'inégalité est encore vraie lorsque $n = 7$ ou 8, en calculant :

$$\begin{cases} \Delta_7 = \text{ppcm}\,(1,2,3,4,5,6,7) = 2^2 \times 3 \times 5 \times 7 = 420 \geq 2^7 = 128 \\ \Delta_8 = \text{ppcm}(\Delta_7, 8) = \text{ppcm}(420, 8) = 840 \geq 2^8 = 256. \end{cases}$$

A.I.5.a. Comme $\Delta_n = \text{ppcm}\,(1, \ldots, n)$,

$$v_p\,(\Delta_n) = \text{Max}\,\{v_p\,(i)\ /\ i \in \{1, \ldots, n\}\}$$

et il existe $k \in \{1, \ldots, n\}$ tel que $v_p\,(\Delta_n) = v_p\,(k)$. Mais alors

$$p^{v_p(k)} \leq k = \prod_{q \in \mathcal{P}} q^{v_q(k)} \leq n$$

montre bien que $p^{v_p(\Delta_n)} \leq n$.

A.I.5.b. On a toujours $\Delta_n = \prod_{p\in\mathcal{P}} p^{v_p(\Delta_n)}$, et il s'agit de montrer que, dans ce produit, les seuls nombres premiers qui interviennent réellement sont tels que $p \leq n$, autrement dit que :

$$p > n \ \Rightarrow \ v_p\left(\Delta_n\right) = 0.$$

Raisonnons par l'absurde, et supposons qu'il existe $p \in \mathcal{P}$ tel que $p > n$ et $v_p\left(\Delta_n\right) \geq 1$. Le a) permet d'écrire $n < p \leq p^{v_p(\Delta_n)} \leq n$, ce qui est absurde.

A.I.5.c. On utilise les deux questions précédentes pour écrire :

$$\Delta_n = \prod_{p\leq n} p^{v_p(\Delta_n)} \leq \prod_{p\leq n} n = n^{\pi(n)}.$$

puisque le produit $\prod_{p\leq n} n = n \times n \times ... \times n$ possède $\pi(n)$ facteurs.

A.I.6.a. En utilisant A.I.4.f et A.I.5.c, on obtient :

$$\forall n \geq 7 \quad 2^n \leq \Delta_n \leq n^{\pi(n)},$$

d'où $n \ln 2 \leq \pi(n) \ln n$, et

$$\forall n \geq 7 \quad (\ln 2)\frac{n}{\ln n} \leq \pi(n). \quad (3)$$

A.I.6.b. On pose $\varphi\left(n\right) = \left(\ln 2\right) n/\ln n$ et on complète le tableau suivant en utilisant notre calculatrice :

n	2	3	4	5	6
$\varphi\left(n\right)$	2	$1,89$	$2,00$	$2,15$	$2,32$
$\pi(n)$	1	2	2	3	3

L'inégalité (3) est donc vraie pour tout $n \geq 2$.

II. Une majoration de la fonction π

A.II.1.a. Posons

$$c = \binom{b}{a} = \frac{b!}{a!\left(b-a\right)!} = \frac{b\left(b-1\right)...\left(b-a+1\right)}{a!}.$$

c est entier et

$$a! \times c = b\left(b-1\right)...\left(b-a+1\right).$$

Comme tous les p qui interviennent dans le produit $\prod_{a<p\leq b} p$ sont premiers, montrer que $\prod_{a<p\leq b} p$ divise c revient à montrer que

$$\forall p \in \mathcal{P} \cap]a,b] \quad p \text{ divise } c,$$

et c'est ce que nous allons démontrer.
Si $p \in \mathcal{P} \cap]a,b]$, l'hypothèse $b/2 \leq a$ donne $b \leq 2a$, soit $b-a+1 \leq a+1$. Le produit $b\,(b-1)\ldots(b-a+1)$ contient donc tous les entiers situés dans l'intervalle $]a,b]$, et en particulier p. On en déduit que p divise $b\,(b-1)\ldots(b-a+1)$, autrement dit que p divise $a! \times c$.
Mais p est premier, donc premier avec tout nombre qu'il ne divise pas. Comme $p > a$, p ne peut diviser aucun facteur du produit $a!$, donc ne peut pas diviser $a!$. Donc p est premier avec $a!$, et comme p divise $a! \times c$, le Théorème de Gauss montre que p divise c. Cela achève la preuve.

A.II.1.b. On applique le résultat de la question précédente avec $a = m+1$ et $b = 2m+1$. La seule chose à bien vérifier[13] est que l'hypothèse $0 < \frac{b}{2} \leq a < b$ est satisfaite. On a bien

$$\frac{b}{2} = m + \frac{1}{2} \leq a = m+1 \quad \text{et} \quad a = m+1 < b = 2m+1$$

puisque $m \geq 1$. On peut alors dire que $\prod_{m+1<p\leq 2m+1} p$ divise $\binom{2m+1}{m+1}$.

A.II.1.c. De façon générale, on sait que $\binom{b}{a} = \binom{b}{b-a}$, ce qui donne ici

$$\binom{2m+1}{m} = \binom{2m+1}{m+1}.$$

Un calcul direct le confirme :

$$\binom{2m+1}{m} = \frac{(2m+1)!}{m! \times (m+1)!} = \binom{2m+1}{m+1}.$$

A.II.1.d. On a

$$4^m \times 2 = (1+1)^{2m+1} = \sum_{k=0}^{2m+1} \binom{2m+1}{k} = 2\sum_{k=0}^{m} \binom{2m+1}{k}$$

si l'on tient compte de la symétrie des coefficients binomiaux suivant laquelle $\binom{2m+1}{k} = \binom{2m+1}{2m+1-k}$ pour tout $k \in [0,m]$. Par suite

$$4^m = \sum_{k=0}^{m} \binom{2m+1}{k}.$$

[13] Cette vérification est primordiale : ne pas la faire donne zéro à la question, car c'est la seule difficulté de celle-ci !

Comme tous les termes de la somme sont positifs, chacun de ces termes sera inférieur à 4^m, et en particulier quand $k = m$:

$$\forall m \geq 1 \quad \binom{2m+1}{m} \leq 4^m$$

A.II.1.e. D'après A.II.1.b, $\prod_{m+1<p\leq 2m+1} p$ divise $\binom{2m+1}{m+1}$, donc est inférieur à ce nombre. Les trois questions précédentes permettent donc d'écrire :

$$\prod_{m+1<p\leq 2m+1} p \leq \binom{2m+1}{m+1} = \binom{2m+1}{m} \leq 4^m.$$

A.II.1.f. • La propriété P_1 est vrai puisque, si $k = 1$,

$$\prod_{p\leq k} p = \prod_{p\leq 1} p = 1 \leq 4^k = 4^1.$$

• La propriété P_2 est vrai puisque, si $k \in \{1, 2, 3, 4\}$, alors $\prod_{p\leq k} p \leq 4^k$. Je ne ferai qu'une vérification, les autres étant du même acabit. Par exemple, pour $k = 3$, j'obtiens $\prod_{p\leq 3} p = 2 \times 3 = 6$ qui est bien inférieur à $4^3 = 64$.

• Supposons que la propriété P_n soit vraie, avec $n \geq 2$, et montrons que la propriété P_{n+1} est encore vraie. Il faut prouver que :

$$\forall k \in \{1, ..., 2n+2\} \quad \prod_{p\leq k} p \leq 4^k.$$

Il n'y a rien à démontrer si $k \in \{1, ..., 2n\}$, puisque l'inégalité provient alors de l'application de la propriété de récurrence au rang n. Il nous faut seulement vérifier que

$$\forall k \in \{2n+1, 2n+2\} \quad \prod_{p\leq k} p \leq 4^k. \quad (\natural)$$

On remarque que $2n + 2$ n'est pas premier (c'est le produit de 2 et de $n + 1$ qui n'est pas égal à 1), donc que

$$\{p \in \mathcal{P} \,/\, 0 \leq p \leq 2n+1\} = \{p \in \mathcal{P} \,/\, 0 \leq p \leq 2n+2\},$$

et que $\prod_{p\leq 2n+1} p = \prod_{p\leq 2n+2} p$. Pour démontrer ($\natural$), il suffit donc de montrer que

$$\prod_{p\leq 2n+1} p \leq 4^{2n+1}.$$

On écrit

$$\prod_{p\leq 2n+1} p = \prod_{p\leq n+1} p \times \prod_{n+1<p\leq 2n+1} p. \quad (\flat)$$

L'hypothèse P_n au rang n donne $\prod_{p\leq n+1} p \leq 4^{n+1}$ (on a bien $2n+1 \leq 2n$ donc P_n s'applique). La question A.II.1.e donne $\prod_{n+1<p\leq 2n+1} p \leq 4^n$. En reportant dans ($\flat$), on obtient :

$$\prod_{p\leq 2n+1} p = \prod_{p\leq n+1} p \times \prod_{n+1<p\leq 2n+1} p \leq 4^{n+1} \times 4^n = 4^{2n+1},$$

comme désiré.

A.II.2.a. $e^m = \sum_{k=0}^{+\infty} \frac{m^k}{k!}$ est la somme d'une série entière à termes strictement positifs, donc

$$\frac{m^m}{m!} < e^m, \quad \text{d'où} \quad \left(\frac{m}{e}\right)^m < m!.$$

A.II.2.b. • On vérifie que

$$\pi(n)! \leq \prod_{p\leq n} p \leq 4^n.$$

La seconde inégalité $\prod_{p\leq n} p \leq 4^n$ a été montrée en A.II.1.f. Pour montrer la première inégalité, on écrit

$$\prod_{p\leq n} p = p_1 \times p_2 \times ... \times p_{\pi(n)},$$

où les nombres premiers p_1, ..., $p_{\pi(n)}$ de l'intervalle $[0,n]$ sont rangés dans l'ordre croissant, et on vérifie que

$$\forall k \in \mathbb{N}^* \quad k \leq p_k$$

par récurrence sur k. La propriété est en effet triviale si $k=1$; et si on la suppose vraie au rang k, on obtient $k+1 \leq p_k + 1 \leq p_{k+1}$ puisque la suite d'entiers (p_i) est strictement croissante.
On obtient finalement

$$1 \times 2 \times ... \times (\pi(n)-1) \times \pi(n) \leq \prod_{p\leq n} p = p_1 \times p_2 \times ... \times p_{\pi(n)}$$

c'est-à-dire $\pi(n)! \leq \prod_{p\leq n} p$.

• L'inégalité précédente et celle montrée dans la question A.II.2.a donnent

$$\left(\frac{\pi(n)}{e}\right)^{\pi(n)} < \pi(n)! \leq 4^n$$

d'où $\pi(n)(\ln \pi(n) - \ln e) \leq n \ln 4$, c'est-à-dire $\pi(n) \ln \pi(n) - \pi(n) \leq n \ln 4$.

A.II.3.a. • La fonction $\varphi : x \mapsto x \ln x - x$ est définie et continue sur $\mathbb{R}_+^*$, dérivable sur $\mathbb{R}_+^*$, et de nombre-dérivé $\varphi'(x) = \ln x$ strictement positif pour tout $x > 1$. Il s'ensuit que φ est strictement croissante sur $[1, +\infty[$.

• Par hypothèse

$$e \frac{n_0}{\ln n_0} < \pi(n_0).$$

Comme $e \frac{n_0}{\ln n_0} \geq e \frac{3}{\ln 3} \simeq 7,4 \geq 1$, la croissance stricte de f sur $[1, +\infty[$ et la question A.II.2.b donnent

$$e \frac{n_0}{\ln n_0} \ln \left(e \frac{n_0}{\ln n_0} \right) - e \frac{n_0}{\ln n_0} < \pi(n_0) \ln \pi(n_0) - \pi(n_0) \leq n_0 \ln 4$$

$$\frac{e}{\ln n_0} (1 + \ln n_0 - \ln \ln n_0) - \frac{e}{\ln n_0} < \ln 4$$

$$e - e \frac{\ln \ln n_0}{\ln n_0} < \ln 4$$

soit

$$\frac{e - \ln 4}{e} < \frac{\ln \ln n_0}{\ln n_0}.$$

A.II.3.b. • L'application $\psi : [1, +\infty[\to \mathbb{R}$ qui à x associe $\psi(x) = \frac{1}{e} - \frac{\ln x}{x}$ est définie et dérivable sur $[1, +\infty[$, de dérivée $\psi'(x) = \frac{\ln x - 1}{x^2}$.
$\psi'(x)$ s'annule seulement en e, et

$$\psi'(x) \geq 0 \iff \ln x \geq 1 \iff x \geq e.$$

Donc ψ admet un minimum absolu en e, et

$$\forall x \in [1, +\infty[\quad \psi(e) = 0 \leq \psi(x),$$

c'est-à-dire

$$\forall x \in [1, +\infty[\quad \frac{\ln x}{x} < \frac{1}{e}.$$

• Finalement

$$\frac{e - \ln 4}{e} < \frac{\ln \ln n_0}{\ln n_0} < \frac{1}{e}$$

donc $e < \ln 4$, ce qui est absurde puisque $\ln 4 \simeq 1,38$.

Partie B : AUTOUR D'UN THEOREME DE MERTENS

I. Une formule de Legendre sur la valuation p-adique de $n!$

B.I.1. • La partie $E = \left\{k \in \mathbb{N} \,/\, n < p^k\right\}$ est incluse dans $\mathbb{N}$, et non vide (puisque $\lim_{k\to+\infty} p^k = +\infty$, il existe $P \in \mathbb{N}$ tel que $p \geq P$ entraîne $n < p^k$), donc possède un plus petit élément k_0. Comme $p^0 = 1 \leq n$, p^0 n'appartient pas à E et $k_0 \geq 1$.
On a $p^{k_0-1} \leq n < p^{k_0}$ donc

$$(k_0 - 1)\ln p \leq \ln n < k_0 \ln p$$

$$k_0 - 1 \leq \frac{\ln n}{\ln p} < k_0,$$

de sorte que $k_0 = \left[\dfrac{\ln n}{\ln p}\right] + 1$.

B.I.2.a. Si $a \in \{1, ..., n\}$,

$$a \in U_{k+1} \quad \Leftrightarrow \quad p^{k+1} \mid a \quad \Rightarrow \quad p^k \mid a \quad \Leftrightarrow \quad a \in U_k$$

donc $U_{k+1} \subset U_k$. L'entier p^k appartient à $\{1, ..., n\}$ dès que $k \in \{0, ..., k_0 - 1\}$, est divisible par p^k mais pas par p^{k+1}, donc appartient à $U_k \backslash U_{k+1}$. L'inclusion $U_{k+1} \subset U_k$ est donc stricte.
Si $k \geq k_0$, p^k ne peut diviser aucun nombre compris entre 1 et n (puisque $n < p^{k_0} \leq p^k$) donc $U_k = \varnothing$.

B.I.2.b. Si $a \in \{1, ..., n\}$,

$$a \in V_k \quad \Leftrightarrow \quad p^k \text{ ne divise pas } a \quad \Rightarrow \quad p^{k+1} \text{ ne divise pas } a \quad \Leftrightarrow \quad a \in V_{k+1}$$

donc $V_k \subset V_{k+1}$. Cette inclusion est stricte puisque p^k est un élément de $\{1, ..., n\}$ divisible par p^k mais pas par p^{k+1}, donc $p^k \in V_{k+1} \backslash V_k$. Si $k \geq k_0$, p^k ne divise aucun nombre entier de l'intervalle $[1, n]$ (car $n < p^{k_0} \leq p^k$), donc $V_k = \{1, ..., n\}$.

B.I.2.c. Il s'agit de vérifier les trois points suivants :

• Aucune des parties Ω_k n'est vide : comme $k \in \{0, ..., k_0 - 1\}$, p^k est de valuation k et appartient à $\{1, ..., n\}$, donc appartient à Ω_k.

• L'intersection $\Omega_k \cap \Omega_l$ de deux éléments de la famille est toujours vide, puisqu'un entier a ne possède qu'une seule valuation p-adique $v_p(a)$.

• On a $\{1, ..., n\} = \bigcup_{k=0}^{k_0-1} \Omega_k$. En effet, si $a \in \{1, ..., n\}$, il existe $k \in \mathbb{N}$, et un entier naturel q premier avec p, tels que $a = p^k q$. Dans ce cas $v_p(a) = k$, et il est facile de voir que $k \leq k_0 - 1$ (par l'absurde : si $k \geq k_0$, alors $a = p^k q \geq p^{k_0} > n$, absurde), d'où $a \in \Omega_k$. Cela montre que

$$\{1, ..., n\} \subset \bigcup_{k=0}^{k_0-1} \Omega_k,$$

et l'inclusion réciproque est triviale !

B.I.3.a. Pour tout k, les équivalences

$$a \in \Omega_k \ \Leftrightarrow\ v_p(a) = k \ \Leftrightarrow\ \begin{cases} p^k \mid a \\ p^{k+1} \nmid a \end{cases} \Leftrightarrow\ a \in U_k \cap V_{k+1},$$

montrent que $\Omega_k = U_k \cap V_{k+1}$.

B.I.3.b. • On a

$$\begin{aligned} a \in U_k &\Leftrightarrow \left(a = p^k q \ \text{ et } \ 1 \leq p^k q \leq n\right) \\ &\Leftrightarrow \left(a = p^k q \ \text{ et } \ 1 \leq q \leq \frac{n}{p^k}\right) \end{aligned}$$

donc $|U_k| = \left[\dfrac{n}{p^k}\right]$.

Remarque : Je noterai $|E|$ au lieu de $\#E$ le cardinal de l'ensemble E.

• Comme $V_k = \{1, ..., n\} \setminus U_k$,

$$|V_k| = n - |U_k| = n - \left[\frac{n}{p^k}\right].$$

• On a

$$\begin{aligned} a \in \Omega_k &\Leftrightarrow \left(a = p^k q \ \text{ et } \ 1 \leq p^k q \leq n \ \text{ et } \ p \nmid q\right) \\ &\Leftrightarrow \left(a = p^k q \ \text{ et } \ 1 \leq q \leq \frac{n}{p^k} \ \text{ et } \ p \nmid q\right). \end{aligned}$$

Il y a $[n/p^k]$ entiers q compris entre 1 et n/p^k. Parmi ceux-ci, combien sont-ils multiples de p ? Dire que q est multiple de p, revient à l'écrire $q = p\alpha$ avec $\alpha \in \mathbb{N}$ et

$$1 \leq p\alpha \leq \frac{n}{p^k},$$

c'est-à-dire

$$1 \leq \alpha \leq \frac{n}{p^{k+1}}.$$

Il y a donc $[\frac{n}{p^{k+1}}]$ entiers q multiples de p et compris entre 1 et n/p^k. On peut donc dire qu'il existe

$$\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^k + 1}\right]$$

entiers q non divisibles par p et compris entre 1 et n/p^k. En conclusion :

$$|\Omega_k| = \left[\frac{n}{p^k}\right] - \left[\frac{n}{p^k + 1}\right].$$

Remarque : On a calculé $|\Omega_k|$ directement sans utiliser les questions précédentes, ce qui était possible. On aurait aussi pu écrire

$$|\Omega_k| = |U_k \cap V_{k+1}| = |U_k| + |V_{k+1}| - |U_k \cup V_{k+1}|$$

et rappeler que $U_{k+1} \subset U_k$ pour en déduire

$$\{1, ..., n\} = U_{k+1} \cup V_{k+1} \subset U_k \cup V_{k+1}$$

soit $U_k \cup V_{k+1} = \{1, ..., n\}$ et $|U_k \cup V_{k+1}| = n$. En reportant, on retrouve

$$|\Omega_k| = \left[\frac{n}{p^k}\right] + \left(n - \left[\frac{n}{p^{k+1}}\right]\right) - n = \left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right].$$

B.I.4. On a $n! = n(n-1)...2 \times 1$ donc

$$v_p(n!) = \sum_{a=1}^{n} v_p(a) = \sum_{k=0}^{k_0-1} \sum_{a \in \Omega_k} v_p(a) = \sum_{k=0}^{k_0-1} k\,|\Omega_k|$$

en utilisant la partition $\{\Omega_0, ..., \Omega_{k_0-1}\}$ de $\{1, ..., n\}$. Par suite

$$v_p(n!) = \sum_{k=1}^{k_0-1} k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^k+1}\right]\right).$$

Posons $u_k = [n/p^k]$. On a

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{k_0-1} k\,(u_k - u_{k+1}) \\ &= (u_1 - u_2) + 2\,(u_2 - u_3) + 3\,(u_3 - u_4) + ... \\ &= u_1 + u_2 + u_3 + ... + u_{k_0-1} - (k_0 - 1)\,u_{k_0}. \end{aligned}$$

Comme $u_{k_0} = u_{k_0+1} = ... = 0$,

$$v_p(n!) = \sum_{k=1}^{k_0-1} u_k = \sum_{k=1}^{k_0-1} \left[\frac{n}{p^k}\right] = \sum_{k \geq 1} \left[\frac{n}{p^k}\right].$$

Remarque : On peut dire les choses différemment, par exemple écrire

$$\begin{aligned} v_p(n!) &= \sum_{k=1}^{k_0-1} k\left(u_k - u_{k+1}\right) \\ &= \sum_{k=1}^{k_0-1} k u_k - \sum_{k=1}^{k_0-1} k u_{k+1} \\ &= \sum_{k=1}^{k_0-1} k u_k - \sum_{k'=2}^{k_0} \left(k'-1\right) u_{k'} \\ &= u_1 + \sum_{k=2}^{k_0-1} \left(k-(k-1)\right) u_k \ = \ \sum_{k=1}^{k_0-1} u_k. \end{aligned}$$

II. Un théorème de Mertens

B.II.1. On obtient

$$\frac{n}{p} - 1 < \left[\frac{n}{p}\right] \leq v_p(n!) = \sum_{k\geq 1}\left[\frac{n}{p^k}\right] \leq \sum_{k\geq 1}\frac{n}{p^k}.$$

Comme

$$\sum_{k\geq 1}\frac{n}{p^k} = n\times\frac{1}{p}\times\frac{1}{1-\frac{1}{p}} = \frac{n}{p-1} = \frac{n}{p} + \frac{n}{p\left(p-1\right)},$$

on obtient bien $\frac{n}{p} - 1 < v_p(n!) \leq \frac{n}{p} + \frac{n}{p\left(p-1\right)}$.

B.II.2. Si p est premier et divise $n!$, il divise l'un des facteurs 1, 2, ..., n de $n!$ donc $p \leq n$. Ainsi $v_p(n!) = 0$ dès que $p > n$, et $n! = \prod_{p\leq n} p^{v_p(n!)}$. En utilisant la question précédente, on obtient

$$\sum_{p\leq n}\left(\frac{n}{p}-1\right)\ln p < \ln n! = \sum_{p\leq n} v_p(n!)\ln p \leq \sum_{p\leq n}\left(\frac{n}{p}+\frac{n}{p\left(p-1\right)}\right)\ln p$$

soit

$$n\sum_{p\leq n}\frac{\ln p}{p} - \sum_{p\leq n}\ln p < \ln n! \leq n\sum_{p\leq n}\frac{\ln p}{p} + n\sum_{p\leq n}\frac{\ln p}{p\left(p-1\right)}.$$

B.II.3.a. Considérons la série entière $\sum_{k\geq 0} x^k/2^k$. Si $a_k = 1/2^k$,

$$\lim\frac{|a_{k+1}|}{|a_k|} = \lim\frac{2^k}{2^{k+1}} = \frac{1}{2}$$

donc le rayon de convergence de $\sum_{k\geq 0} x^k/2^k$ est 2. La série converge absolument en tout point x de $]-2,2[$ vers un réel $S(x)$. D'après le cours, $x \mapsto S(x)$ est une application dérivable sur $]-2,2[$, la série entière $\sum_{k\geq 1} kx^{k-1}/2^k$ est encore de rayon de convergence 2 donc converge absolument en tout point de cet intervalle (en particulier $\sum_{r\geq 1} r/2^r$ converge), et

$$\forall x \in]-2,2[\quad S'(x) = \sum_{k\geq 1} \frac{kx^{k-1}}{2^k}.$$

Mais

$$S(x) = \sum_{k\geq 0} \frac{x^k}{2^k} = \frac{1}{1-x/2} = \frac{2}{2-x},$$

donc $S'(x) = \frac{2}{(2-x)^2}$, si bien que

$$\forall x \in]-2,2[\quad \sum_{k\geq 1} \frac{kx^{k-1}}{2^k} = \frac{2}{(2-x)^2}.$$

En prenant $x=1$, on obtient bien $\displaystyle\sum_{k\geq 1} \frac{k}{2^k} = 2$.

B.II.3.b. On a

$$\sum_{2^{r-1}<m\leq 2^r} \frac{1}{m(m-1)} = \sum_{2^{r-1}<m\leq 2^r} \left(\frac{1}{m-1} - \frac{1}{m}\right) = \frac{1}{2^{r-1}} - \frac{1}{2^r} = \frac{1}{2^r},$$

donc $$U_r = \sum_{2^{r-1}<m\leq 2^r} \frac{\ln m}{m(m-1)} \leq \sum_{2^{r-1}<m\leq 2^r} \frac{\ln(2^r)}{m(m-1)} = \frac{r}{2^r}\ln 2.$$

B.II.3.c. Chaque terme de la série à termes positifs $\sum_{r\geq 1} U_r$ est majoré par $\dfrac{r}{2^r}\ln 2$, et la série $\sum_{r\geq 1} \dfrac{r}{2^r}\ln 2$ converge vers $2\ln 2$ d'après B.II.3.a, donc $\sum_{r\geq 1} U_r$ converge et sa somme est $\leq 2\ln 2$.

Remarque : On peut "maquiller" la solution différemment, sans faire appel aux résultats du cours concernant les séries à termes positifs, donc en retournant au suite (ce qui revient à justifier ces résultats du cours). Ainsi, la suite $(\sum_{r=1}^{R} U_r)_R$ est croissante, et majorée puisque pour tout R,

$$\sum_{r=1}^{R} U_r \leq \sum_{r=1}^{R} \frac{r}{2^r}\ln 2 \leq (\ln 2)\sum_{r=1}^{+\infty} \frac{r}{2^r} = 2\ln 2,$$

donc convergente dans $\mathbb{R}$. Cela signifie que la série $\sum_{r\geq 1} U_r$ converge et que $\sum_{r=1}^{+\infty} U_r \leq \ln 4$.

B.II.3.d. La série $\sum_{m\geq 2} \frac{\ln m}{m(m-1)}$ est à termes positifs, donc la suite associée $(\sum_{m=2}^{M} \frac{\ln m}{m(m-1)})_M$ est croissante. Montrer qu'une telle suite converge dans $\mathbb{R}$ revient donc à montrer qu'elle est majorée. C'est immédiat : pour tout entier $M \geq 2$, il existe un entier R tel que $M \leq 2^R$, et

$$\sum_{m=2}^{M} \frac{\ln m}{m\,(m-1)} \leq \sum_{m=2}^{2^R} \frac{\ln m}{m\,(m-1)} \leq \sum_{r=1}^{R} \sum_{2^{r-1}<m\leq 2^r} \frac{\ln m}{m\,(m-1)}$$

donc

$$\sum_{m=2}^{M} \frac{\ln m}{m\,(m-1)} \leq \sum_{r=1}^{R} U_r \leq \sum_{r=1}^{+\infty} U_r \leq \ln 4.$$

On obtient de surcroît la majoration

$$\sum_{m=2}^{+\infty} \frac{\ln m}{m\,(m-1)} \leq \ln 4.$$

B.II.3.e. Les fonctions[14] $\xi\,(u) = \ln(1+u) - u + \frac{u^2}{2}$ et $\zeta\,(u) = u - \ln(1+u)$ sont définies et dérivables sur $]-1,+\infty[$, de dérivées

$$\xi'\,(u) = \frac{1}{1+u} - 1 + u = \frac{u^2}{1+u} \quad \text{et} \quad \zeta'\,(u) = 1 - \frac{1}{1+u} = \frac{u}{1+u}$$

positives sur $[0,+\infty[$. Ce sont donc des fonctions croissantes sur $[0,+\infty[$, et pour tout $x \geq 0$, $\xi\,(u) \geq \xi\,(0) = 0$ et $\zeta\,(u) \geq \zeta\,(0) = 0$, c'est-à-dire

$$\forall u \in \mathbb{R}_+ \quad u - \frac{u^2}{2} \leq \ln(1+u) \leq u.$$

En faisant $u = 1/n$, on trouve

$$\forall n \in \mathbb{N}^* \quad 1 - \frac{1}{2n} \leq n\ln(1+\frac{1}{n}) \leq 1$$

et

$$\forall n \in \mathbb{N}^* \quad \frac{1}{2n} \leq \frac{1}{n} - \frac{1}{2n^2} \leq \ln(1+\frac{1}{n}),$$

[14] Par commodité, je me permets d'identifier l'image d'un point par une fonction et la fonction elle-même, ce qui est certes abusif, mais très pratique et inoffensif si l'on sait exactement de quel abus il s'agit. Un tel abus, qui correspond à un usage courant, doit pouvoir être expliqué sereinement à l'oral si des explications sont demandées par le jury. A l'écrit, on peut glisser une note pour signaler l'abus sans s'apesantir.

puisque l'inégalité $\frac{1}{2n} \leq \frac{1}{n} - \frac{1}{2n^2}$ est facile à vérifier (elle équivaut à $n^2 \geq n$).

B.II.3.f. La propriété est vraie au rang $n = 1$ en prenant n'importe quel réel θ_1 dans l'intervalle $[0, 1]$ puisqu'on a toujours $\ln 1 = 1 \ln 1 - 1 + 1 + \theta_1 \ln 1$. Si la propriété est vraie au rang n, montrons-là au rang $n + 1$. On a

$$\begin{aligned}\ln (n+1)! &= \ln (n+1) + \ln n! \\ &= \ln (n+1) + n \ln n - n + 1 + \theta_n \ln n,\end{aligned}$$

et on aura

$$\ln (n+1)! = (n+1) \ln (n+1) - (n+1) + 1 + \theta_{n+1} \ln (n+1)$$

si et seulement si θ_{n+1} vérifie

$$\ln (n+1) + n \ln n - n + 1 + \theta_n \ln n = (n+1) \ln (n+1) - n + \theta_{n+1} \ln (n+1)$$

autrement dit, si et seulement si,

$$\begin{aligned}\theta_{n+1} \ln (n+1) &= n \ln n - n \ln (n+1) + 1 + \theta_n \ln n \\ &= 1 + \theta_n \ln n - n \ln(1 + \frac{1}{n}).\end{aligned}$$

Le seul réel θ_{n+1} qui convienne est donc

$$\theta_{n+1} = \frac{1}{\ln (n+1)} \left[1 + \theta_n \ln n - n \ln(1 + \frac{1}{n}) \right]$$

et nous devons juste vérifier que $\theta_{n+1} \in [0, 1]$ pour conclure.

▶ On a

$$0 \leq \theta_{n+1} \quad \Leftrightarrow \quad n \ln(1 + \frac{1}{n}) \leq 1 + \theta_n \ln n$$

et la dernière inégalité écrite est vraie puisqu'en utilisant la question précédente,

$$n \ln(1 + \frac{1}{n}) \leq 1 \leq 1 + \theta_n \ln n.$$

▶ On a

$$\begin{aligned}\theta_{n+1} \leq 1 &\Leftrightarrow 1 + \theta_n \ln n - n \ln(1 + \frac{1}{n}) \leq \ln (n+1) \\ &\Leftrightarrow 1 + \theta_n \ln n - \ln (n+1) \leq n \ln(1 + \frac{1}{n}). \quad (*)\end{aligned}$$

La question précédente permet d'écrire

$$n \ln(1 + \frac{1}{n}) \geq 1 - \frac{1}{2n} \geq 1 - \ln(1 + \frac{1}{n}) \geq 1 + \ln n - \ln (n+1)\,.$$

Comme $\theta_n \leq 1$, on a aussi

$$1 + \theta_n \ln n - \ln(n+1) \leq 1 + \ln n - \ln(n+1),$$

et l'on obtient bien $(*)$ en mettant ces inégalités bout à bout.

B.II.4. • D'après B.II.2 et B.II.3.d,

$$\begin{aligned}\sum_{p\leq n} \frac{\ln p}{p} &\geq \frac{\ln n!}{n} - \sum_{p\leq n} \frac{\ln p}{p(p-1)} \\ &\geq \frac{\ln n!}{n} - \sum_{m=2}^{+\infty} \frac{\ln m}{m(m-1)} \geq \frac{\ln n!}{n} - \ln 4,\end{aligned}$$

et en utilisant B.II.3.f,

$$\sum_{p\leq n} \frac{\ln p}{p} \geq \ln n - 1 + \frac{1}{n} + \theta_n \frac{\ln n}{n} - \ln 4 \geq \ln n - (1 + \ln 4).$$

B.II.5. D'après B.II.2,

$$\sum_{p\leq n} \frac{\ln p}{p} \leq \frac{\ln n!}{n} + \frac{1}{n} \sum_{p\leq n} \ln p.$$

La question A.II.1.f donne $\sum_{p\leq n} \ln p = \ln\left(\prod_{p\leq n} p\right) \leq \ln 4^n$, donc

$$\sum_{p\leq n} \frac{\ln p}{p} \leq \frac{\ln n!}{n} + \ln 4.$$

En utilisant B.II.3.f, on obtient

$$\begin{aligned}\sum_{p\leq n} \frac{\ln p}{p} &\leq \ln n - 1 + \frac{1}{n} + \theta_n \frac{\ln n}{n} + \ln 4 \\ &\leq \ln n - 1 + \frac{1}{n} + \frac{\ln n}{n} + \ln 4.\end{aligned}$$

Pour obtenir $\sum_{p\leq n} \frac{\ln p}{p} \leq \ln n + \ln 4$, il suffit de vérifier l'inégalité

$$\ln n - 1 + \frac{1}{n} + \frac{\ln n}{n} + \ln 4 \leq \ln n + \ln 4$$

qui s'écrit $\dfrac{\ln n}{n} \leq 1 - \dfrac{1}{n}$, ou encore $\ln n \leq n - 1$. Cette dernière égalité est vraie comme on le voit en faisant $u = n - 1$ dans l'inégalité $\ln(1+u) \leq u$ démontrée en B.II.3.e. En conclusion

$$\sum_{p \leq n} \frac{\ln p}{p} \leq \ln n + \ln 4.$$

• Finalement

$$\forall n \in \mathbb{N}^* \backslash \{2\} \quad -(1 + \ln 4) \leq \sum_{p \leq n} \frac{\ln p}{p} - \ln n \leq \ln 4$$

donc

$$\forall n \in \mathbb{N}^* \backslash \{2\} \quad \left| \sum_{p \leq n} \frac{\ln p}{p} - \ln n \right| \leq 1 + \ln 4.$$

Cela signifie que

$$\sum_{p \leq n} \frac{\ln p}{p} - \ln n = O(1)$$

comme on le désirait.

Remarque : La formule de Mertens que l'on vient de montrer implique que $\sum_{p \leq n} \frac{\ln p}{p}$ est équivalent à $\ln n$ quand n tend vers $+\infty$. En effet, si (u_n) et (v_n) sont deux suites qui tendent vers $+\infty$ et telles que $u_n - v_n = O(1)$, alors

$$\frac{u_n}{v_n} - 1 = \frac{O(1)}{v_n}$$

donc $\lim(u_n/v_n) = 1$, c'est-à-dire $u_n \sim v_n$.

III. Le comportement asymptotique de $\left(\sum_{p \leq n} \frac{1}{p}\right)_n$

B.III.1.a. Les fonctions $f(x) = 1/x \ln^2 x$ et $g(x) = 1/x \ln x$ sont continues positives et décroissantes sur $[2, +\infty[$. On a donc, pour tout $k \in \mathbb{N}^* \backslash \{1\}$,

$$f(k+1) \leq \int_k^{k+1} f(x)\, dx \leq f(k)$$

et en sommant

$$\sum_{k=2}^{K} f(k+1) \leq \int_2^{K+1} f(x)\, dx \leq \sum_{k=2}^{K} f(k) \quad (*)$$

pour tout $K \in \mathbb{N}^*\setminus\{1\}$, et la même chose avec g à la place de f.

• Comme

$$\left(\frac{1}{\ln^2 x}\right)' = -\frac{1}{\ln^4 x} \times 2\ln x \times \frac{1}{x} = -\frac{2}{x\ln^3 x},$$

et comme les fonctions $\frac{1}{x}$ et $\frac{1}{\ln^2 x}$ sont de classe C^1 sur $[2,+\infty[$, une intégration par parties donne

$$\begin{aligned}\int_2^A f(x)\ dx &= \int_2^A \frac{1}{x\ln^2 x}\,dx \\ &= \left[\frac{1}{\ln x}\right]_2^A - \int_2^A \ln x\left(-\frac{2}{x\ln^3 x}\right)dx \\ &= \frac{1}{\ln A} - \frac{1}{\ln 2} + 2\int_2^A \frac{1}{x\ln^2 x}\,dx\end{aligned}$$

soit

$$\int_2^A f(x)\ dx = \frac{1}{\ln 2} - \frac{1}{\ln A}.$$

En passant à la limite quand A tend vers $+\infty$, on constate que la limite de $\int_2^A f(x)\ dx$ existe et vaut $1/\ln 2$. L'intégrale généralisée $\int_2^{+\infty} f(x)\ dx$ est donc convergente et

$$\int_2^{+\infty} f(x)\ dx = \frac{1}{\ln 2}.$$

Les inégalités $(*)$ donnent alors

$$\sum_{k=2}^{K} f(k+1) \le \int_2^{K+1} f(x)\ dx \le \frac{1}{\ln 2}$$

pour tout K. Cela montre que la suite croissante $\left(\sum_{k=2}^{K} f(k+1)\right)_K$ est majorée par $1/\ln 2$, donc converge vers une limite inférieure à $1/\ln 2$, et que, par conséquent, la série $\sum 1/n\ln^2 n$ converge.

• Le changement de variables $u = \ln x$ donne

$$\int_2^A g(x)\ dx = \int_2^A \frac{1}{x\ln x}\,dx = \int_2^A \frac{1}{u}\,du = \ln A - \ln 2.$$

Par suite $\lim_{A\to+\infty} \int_2^A g(x)\ dx = \lim_{A\to+\infty} (\ln A - \ln 2) = +\infty$ et l'intégrale $\int_2^{+\infty} g(x)\ dx$ diverge. On en déduit que, pour tout $S \in \mathbb{R}$ il existe $K \in \mathbb{N}^*\setminus\{1\}$ tel que

$$S \le \int_2^{K+1} g(x)\ dx.$$

En utilisant les inégalités $(*)$, on trouve

$$\forall S \in \mathbb{R} \quad \exists K \in \mathbb{N}^* \backslash \{1\} \quad S \leq \int_2^{K+1} g(x)\, dx \leq \sum_{k=2}^{K} g(k),$$

ce qui montre que la suite $\left(\sum_{k=2}^{K} g(k)\right)_K$ tend vers $+\infty$ quand K tend vers $+\infty$. La série $\sum 1/n \ln n$ est donc divergente.

- Avec g, les inégalités $(*)$ s'écrivent

$$\sum_{k=2}^{K} \frac{1}{(k+1)\ln(k+1)} \leq \int_2^{K+1} \frac{1}{x \ln x}\, dx \leq \sum_{k=2}^{K} \frac{1}{k \ln k}$$

soit

$$\frac{1}{(K+1)\ln(K+1)} + \sum_{k=2}^{K} \frac{1}{k \ln k} - \frac{1}{2\ln 2} \leq \int_2^{K+1} \frac{1}{x \ln x}\, dx \leq \sum_{k=2}^{K} \frac{1}{k \ln k}.$$

Comme $\int_2^{K+1} \frac{1}{x \ln x}\, dx = \ln\ln(K+1) - \ln\ln 2$, on obtient a fortiori

$$\ln\ln(K+1) - \ln\ln 2 \leq \sum_{k=2}^{K} \frac{1}{k \ln k} \leq \ln\ln(K+1) - \ln\ln 2 + \frac{1}{2\ln 2}$$

d'où

$$\left| \sum_{k=2}^{K} \frac{1}{k \ln k} - \ln\ln(K+1) \right| \leq \mathrm{Max}\left(|\ln\ln 2|, \left| \ln\ln 2 - \frac{1}{2\ln 2} \right| \right).$$

Cela signifie que $\sum_{k=2}^{K} \frac{1}{k \ln k} = \ln\ln(K+1) + O(1)$, c'est-à-dire

$$\sum_{k=2}^{n-1} \frac{1}{k \ln k} = \ln\ln n + O(1),$$

et on a retrouve la divergence de la série $\sum \frac{1}{n \ln n}$.

Remarques : α) Le dernier point traité permet de se passer de la preuve de la divergence de $\sum \frac{1}{n \ln n}$ donnée au point juste avant.

β) Une section traite des intégrales et séries de Bertrand dans le volume IV de "l'Epreuve d'exposé", dans le chapitre sur la comparaison des fonctions ([19], §. 10.3.3), et la résolution de la question B.III.1 est plus facile si on a revu

les liens entre convergence de séries et convergence d'intégrales généralisées pendant sa préparation ([23], §. 1.6).

B.III.1.b. On a

$$\begin{aligned} u_{n+1} - u_n &= \frac{1}{n \ln n} - \ln \ln (n+1) + \ln \ln n \\ &= \frac{1}{n \ln n} - \ln \left(\frac{\ln (n+1)}{\ln n} \right) . \quad (\maltese) \end{aligned}$$

De $\ln (1 + 1/n) = \ln (n+1) - \ln n$ on tire

$$\begin{aligned} \frac{\ln (n+1)}{\ln n} &= 1 + \frac{\ln \left(1 + \frac{1}{n}\right)}{\ln n} \\ &= 1 + \frac{1}{\ln n} \left(\frac{1}{n} - \frac{1}{2n^2} + o\left(\frac{1}{n^2}\right)\right) \\ &= 1 + \frac{1}{n \ln n} - \frac{1}{2n^2 \ln n} + o\left(\frac{1}{n^2 \ln n}\right) \end{aligned}$$

d'où

$$\begin{aligned} \ln\left(\frac{\ln (n+1)}{\ln n}\right) &= \frac{1}{n \ln n} - \frac{1}{2n^2 \ln n} - \frac{1}{2}\left(\frac{1}{n \ln n} - \frac{1}{2n^2 \ln n}\right)^2 + o\left(\frac{1}{n^2 \ln n}\right) \quad (\blacklozenge) \\ &= \frac{1}{n \ln n} - \frac{1}{2n^2 \ln n} + o\left(\frac{1}{n^2 \ln n}\right) . \end{aligned}$$

En remplaçant dans ($\maltese$),

$$u_{n+1} - u_n = \frac{1}{2n^2 \ln n} + o\left(\frac{1}{n^2 \ln n}\right) .$$

Remarque : A la ligne ($\blacklozenge$), on a redéveloppé $\ln (1 + h)$ à l'ordre 2. Le $o(\frac{1}{n^2 \ln n})$ qui apparaît alors est justifié. On peut le vérifier en notant qu'il aurait dû être signalé comme une somme de fonctions qui sont des $o(\frac{1}{n^2 \ln n})$, des produits issus du développement de

$$-\frac{1}{2}\left(\frac{1}{n \ln n} - \frac{1}{2n^2 \ln n} + o\left(\frac{1}{n^2 \ln n}\right)\right)^2 \quad (\lozenge)$$

et contenant des $o(\frac{1}{n^2 \ln n})$, ou encore un

$$o\left(\left(\frac{1}{n \ln n} - \frac{1}{2n^2 \ln n} + o\left(\frac{1}{n^2 \ln n}\right)\right)^2\right),$$

et que toutes ces fonctions sont négligeables devant $\frac{1}{n^2 \ln n}$. Par exemple, le développement du carré de la ligne ($\lozenge$) contient le terme $\frac{-1}{2n^2 \ln^2 n}$ qui est bien un $o\left(\frac{1}{n^2 \ln n}\right)$ comme on le voit en calculant la limite

$$\lim \frac{-n^2 \ln n}{2n^2 \ln^2 n} = \lim \frac{-1}{2 \ln n} = 0.$$

Cette remarque rassure sans doute, mais il existe une façon plus rapide de justifier la ligne ($\blacklozenge$) : c'est de se référer au cours et annoncer qu'on a effectué une substitution d'un développement limité (on devrait dire ici : développement asymptotique) dans un autre (voir [19], Th. 191, dans le cas de l'échelle de comparaison usuelle relative aux fonctions x^n).

B.III.1.c. La série $\sum \frac{1}{n^2 \ln n}$ est convergente (car son terme général est positif et majoré par $\frac{1}{n^2}$, et que la série de Riemann $\sum \frac{1}{n^2}$ converge). La question précédente montre que

$$u_{n+1} - u_n \sim \frac{1}{2n^2 \ln n}.$$

Comme deux séries à termes positifs équivalents sont de même nature, on en déduit que la série $\sum (u_{n+1} - u_n)$ converge, donc que la suite (u_n) converge vers une limite l. Cela se traduit en écrivant

$$\lim_{n \to +\infty} \left(\sum_{k=2}^{n-1} \frac{1}{k \ln k} - \ln \ln n \right) = l$$

ou encore

$$\sum_{k=2}^{n-1} \frac{1}{k \ln k} = \ln \ln n + l + o(1).$$

B.III.2.a. On peut toujours écrire

$$\sum_{p \leq n} \frac{1}{p} = \sum_{k=2}^{n} \frac{\delta(k) \ln k}{k} . \frac{1}{\ln k}$$

et appliquer la transformation d'Abel avec $a_k = \frac{\delta(k) \ln k}{k}$ et $b_k = \frac{1}{\ln k}$. Avec les notations de l'énoncé,

$$A_n = \sum_{k=2}^{n} a_k = \sum_{k=2}^{n} \frac{\delta(k) \ln k}{k} = \sum_{p \leq n} \frac{\ln p}{p} = \psi(n),$$

et

$$\sum_{p\leq n}\frac{1}{p} = \sum_{k=2}^{n} a_k b_k = A_n b_n + \sum_{k=2}^{n-1} A_k\,(b_k - b_{k+1})$$
$$= \frac{\psi\,(n)}{\ln n} + \sum_{k=2}^{n-1}\psi\,(k)\,(b_k - b_{k+1})\,.$$

Comme

$$b_k - b_{k+1} = \frac{1}{\ln k} - \frac{1}{\ln(k+1)} = \frac{\ln(1+1/k)}{\ln k\ln(k+1)},$$

on obtient bien

$$\sum_{p\leq n}\frac{1}{p} = \sum_{k=2}^{n-1}\psi\,(k)\,\frac{\ln(1+1/k)}{\ln k\ln(k+1)} + \frac{\psi\,(n)}{\ln n}.$$

B.III.2.b. On a

$$\frac{\ln(1+1/k)}{\ln k\ln(k+1)} = \frac{1}{\ln k}\,\frac{t\,(k)}{1+t\,(k)}$$

où $t\,(k)$ est solution de $\ln(1+1/k)\,(1+t\,(k)) = t\,(k)\ln(k+1)$, i.e.

$$t\,(k) = \frac{\ln(1+1/k)}{\ln k}.$$

On a $t\,(k)\sim\frac{1}{k\ln k}$, donc $\lim_{k\to+\infty} t\,(k) = 0$ et

$$\frac{t\,(k)}{1+t\,(k)} = t\,(k)\,(1-t\,(k)+o(t\,(k))) = t\,(k) - t\,(k)^2 + o(t\,(k)^2).$$

Comme

$$\begin{cases} t\,(k) = \dfrac{1}{\ln k}\left(\dfrac{1}{k} - \dfrac{1}{2k^2} + o(\dfrac{1}{k^2})\right) = \dfrac{1}{k\ln k} - \dfrac{1}{2k^2\ln k} + o(\dfrac{1}{k^2\ln k}) \\ t\,(k)^2 \sim \dfrac{1}{k^2\ln^2 k} = o(\dfrac{1}{k^2\ln k}), \end{cases}$$

on obtient

$$\frac{t\,(k)}{1+t\,(k)} = \frac{1}{k\ln k} - \frac{1}{2k^2\ln k} + o(\frac{1}{k^2\ln k}).$$

La formule de Mertens s'écrit $\psi\,(k) = \ln k + O\,(1)$. En reportant :

$$\psi\,(k)\,\frac{\ln(1+1/k)}{\ln k\ln(k+1)} = (\ln k + O\,(1))\left(\frac{1}{k\ln^2 k} - \frac{1}{2k^2\ln^2 k} + o(\frac{1}{k^2\ln^2 k})\right)$$
$$= \frac{1}{k\ln k} + O\left(\frac{1}{k\ln^2 k}\right).$$

Remarque : Cette dernière écriture se vérifie en montrant que tous les monômes obtenus en développant le produit

$$(\ln k + O(1))\left(\frac{1}{k\ln^2 k} - \frac{1}{2k^2\ln^2 k} + o(\frac{1}{k^2\ln^2 k})\right)$$

sont dominés par $\frac{1}{k\ln^2 k}$ (et donc des $O(\frac{1}{k\ln^2 k})$) sauf $\frac{1}{k\ln k}$. Prenons par exemple un de ces monômes au hasard, disons $m(x) = \ln k \times (-\frac{1}{2k^2\ln^2 k}) = -\frac{1}{2k^2\ln k}$, et vérifions que $m(x) = O(\frac{1}{k\ln^2 k})$. On a

$$|m(x)| = \frac{1}{2k^2\ln k} = \frac{1}{k\ln^2 k} \times \frac{\ln k}{2k},$$

et comme $\lim_{k\to+\infty} \frac{\ln k}{2k} = 0$, il existe un entier K tel que

$$k \geq K \quad\Rightarrow\quad \frac{\ln k}{2k} \leq 1 \quad\Rightarrow\quad |m(x)| \leq \frac{1}{k\ln^2 k}.$$

Cela signifie que $m(x) = O(\frac{1}{k\ln^2 k})$.

B.III.3. Les deux questions précédentes donnent

$$\sum_{p\leq n}\frac{1}{p} = \sum_{k=2}^{n-1}\left(\frac{1}{k\ln k} + O\left(\frac{1}{k\ln^2 k}\right)\right) + \frac{\psi(n)}{\ln n}.$$

Le Théorème de Mertens montre que $\frac{\psi(n)}{\ln n} = 1 + o(1)$. En utilisant aussi B.III.1.c, on obtient donc

$$\begin{aligned}\sum_{p\leq n}\frac{1}{p} &= (\ln\ln n + l + o(1)) + \sum_{k=2}^{n-1} v_k + (1 + o(1)) \\ &= \ln\ln n + l + 1 + \sum_{k=2}^{n-1} v_k + o(1)\end{aligned}$$

où (v_k) est une suite telle que $v_k = O(\frac{1}{k\ln^2 k})$, donc telle que la série $\sum_{k=2}^{n-1} v_k$ converge vers un certain réel L (c'est une série absolument convergente puisque $|\frac{1}{k\ln^2 k}| \leq cte \times \frac{1}{k\ln^2 k}$ pour k suffisamment grand et pour une certaine constante cte, et puisque la série $\sum \frac{1}{k\ln^2 k}$ converge d'après la question B.III.1.a). Ainsi $\sum_{k=2}^{n-1} v_k = L + o(1)$, et

$$\sum_{p\leq n}\frac{1}{p} = \ln\ln n + l + 1 + L + o(1) = \ln\ln n + \lambda + o(1)$$

en posant $\lambda = l + 1 + L$.

B.III.4. Appliquons la transformation d'Abel avec la série

$$\sum_{p \leq n} \frac{1}{p} = \sum_{k=2}^{n} \frac{\delta(k)}{k}$$

en posant $a_k = \delta(k)$ et $b_k = 1/k$. On trouve

$$\sum_{p \leq n} \frac{1}{p} = A_n \times \frac{1}{n} + \sum_{k=2}^{n-1} A_k \left(\frac{1}{k} - \frac{1}{k+1} \right)$$

où $A_n = \sum_{k=2}^{n} \delta(k) = \pi(n)$, soit

$$\sum_{p \leq n} \frac{1}{p} = \frac{\pi(n)}{n} + \sum_{k=2}^{n-1} \frac{\pi(k)}{k(k+1)}. \quad (\dagger)$$

Si $\pi(n) \sim c \frac{n}{\ln n}$, alors

$$\frac{\pi(n)}{n} \sim \frac{c}{\ln n}$$

et

$$\frac{\pi(k)}{k(k+1)} \sim \frac{c}{(k+1)\ln k} \sim \frac{c}{k \ln k}.$$

La série $\sum \frac{c}{k \ln k}$ diverge d'après B.III.1.a, et les termes $\frac{\pi(k)}{k(k+1)}$ et $\frac{c}{k \ln k}$ sont tous positifs. On peut donc affirmer que

$$\sum_{k=2}^{n-1} \frac{\pi(k)}{k(k+1)} \sim \sum_{k=2}^{n-1} \frac{c}{k \ln k}$$

en appliquant le Théorème de comparaison des sommes partielles de deux séries divergentes à termes positifs[15]. En utilisant B.III..1.c, on obtient

$$\sum_{k=2}^{n-1} \frac{\pi(k)}{k(k+1)} \sim c \ln \ln n.$$

Dans ce cas, $(\dagger)$ donne

$$\lim \left(\frac{\sum_{p \leq n} \frac{1}{p}}{c \ln \ln n} \right) = \lim \left(\frac{\frac{\pi(n)}{n} + \sum_{k=2}^{n-1} \frac{\pi(k)}{k(k+1)}}{c \ln \ln n} \right) = 1$$

[15] voir [19] Th. 159. Voilà peut-être le moment de traiter la leçon d'oral sur la comparaison des fonctions ([19], Chap. 10) et de regarder d'un peu plus près la Section 10.3.1 d'approfondissement du Vol. IV consacrée à l'intégration et à la sommation des relations de comparaison.

puisque

$$\frac{\frac{\pi(n)}{n}}{c\ln\ln n} \sim \frac{1}{\ln n \times \ln\ln n}$$

tend vers 0 quand n tend vers $+\infty$. Par suite

$$\sum_{p\leq n} \frac{1}{p} \sim c\ln\ln n.$$

Mais B.III.3 donne $\sum_{p\leq n} \frac{1}{p} \sim \ln\ln n$, donc $c\ln\ln n \sim \ln\ln n$. Cela impose à la constante c d'être égale à 1.

IV. Une application à l'étude des entiers possédant de grands facteurs premiers

B.IV.1. En appliquant B.III.3, on trouve

$$\begin{aligned}\sum_{\sqrt{n}\leq p\leq n} \frac{1}{p} &= \sum_{p\leq n} \frac{1}{p} - \sum_{p\leq[\sqrt{n}]} \frac{1}{p} \\ &= \ln\ln n + \lambda + o\left(1\right) - \left(\ln\ln[\sqrt{n}] + \lambda + o\left(1\right)\right) \\ &= \ln\ln n - \ln\ln[\sqrt{n}] + o\left(1\right).\end{aligned}$$

Il ne reste plus qu'à montrer que $L_n = \ln\ln n - \ln\ln[\sqrt{n}]$ tend vers une limite finie quand n tend vers $+\infty$. La croissance de la fonction ln permet d'écrire :

$$\ln\ln\left(\sqrt{n}-1\right) < \ln\ln[\sqrt{n}] \leq \ln\ln\sqrt{n}$$

d'où

$$\ln\ln n - \ln\ln\sqrt{n} \leq L_n < \ln\ln n - \ln\ln\left(\sqrt{n}-1\right).$$

Puisque $\ln\ln\sqrt{n} = \ln(\frac{1}{2}\ln n) = \ln\ln n - \ln 2$, on obtient

$$\ln 2 \leq L_n < \ln\ln n - \ln\ln\left(\sqrt{n}-1\right). \quad (I)$$

Ré-écrivons le membre tout à droite dans ces inégalités. On a

$$\ln\ln\left(\sqrt{n}-1\right) = \ln\ln\sqrt{n}\left(1-\frac{1}{\sqrt{n}}\right) = \ln\left(\ln\sqrt{n} + \ln\left(1-\frac{1}{\sqrt{n}}\right)\right)$$

soit

$$\begin{aligned}\ln\ln\left(\sqrt{n}-1\right) &= \ln\ln\sqrt{n} + \ln\left(1+\frac{\ln\left(1-1/\sqrt{n}\right)}{\ln\sqrt{n}}\right) \\ &= \ln\ln n - \ln 2 + \ln\left(1+\frac{\ln\left(1-1/\sqrt{n}\right)}{\ln\sqrt{n}}\right).\end{aligned}$$

En remplaçant dans (I),

$$\ln 2 \leq L_n < \ln 2 - \ln\left(1 + \frac{\ln(1-1/\sqrt{n})}{\ln\sqrt{n}}\right). \quad (II)$$

Comme

$$\frac{\ln(1-1/\sqrt{n})}{\ln\sqrt{n}} \sim \frac{-2}{\sqrt{n}\times\ln n},$$

on aura $\lim(\frac{\ln(1-1/\sqrt{n})}{\ln\sqrt{n}}) = 0$ donc $\lim\ln(1+\frac{\ln(1-1/\sqrt{n})}{\ln\sqrt{n}}) = 0$. En appliquant le Théorème des gendarmes aux encadrements (II), on obtient finalement $\lim L_n = \ln 2$, donc

$$\lim \sum_{\sqrt{n}\leq p\leq n} \frac{1}{p} = \ln 2.$$

B.IV.2.a. On note que

$$m < p \;\Leftrightarrow\; n = mp < p^2 \;\Leftrightarrow\; \sqrt{n} < p \quad (A1)$$

et que

$$p \leq \frac{x}{m} \;\Leftrightarrow\; mp \leq x \;\Leftrightarrow\; n \leq x. \qquad (A2)$$

Vérifions que

$$\left(p = P^+(n) \text{ et } n \in A(x)\right) \quad\Leftrightarrow\quad m < p \leq \frac{x}{m}.$$

($\Rightarrow$) Par hypothèse $p = P^+(n)$, donc $\sqrt{n} < p$ et $(A1)$ donne $m < p$. Par hypothèse $n \in A(x)$ donc $n \leq x$, et $(A2)$ donne $p \leq x/m$.

($\Leftarrow$) Si $m < p \leq x/m$, il suffit d'appliquer $(A1)$ et $(A2)$ pour avoir

$$\begin{cases} \sqrt{n} < p \\ n \leq x. \end{cases}$$

On vérifie alors :

- que $p = P^+(n)$. En effet, p est un diviseur premier de n, et si q était un diviseur premier de n strictement supérieur à p, q diviserait $n = mp$, donc diviserait m (d'après le Théorème de Gauss), et il existerait $u \in \mathbb{N}$ tel que $m = qu$. Alors $n = pqu > p^2u > nu$ entraînerait $1 > u$, ce qui est absurde.

- que $n \in A(x)$. En effet, $n \leq x$ et $p = P^+(n) > \sqrt{n}$, donc

$$n \in A \cap [0, x] = A(x).$$

B.IV.2.b. La condition est clairement nécessaire. Montrons qu'elle est suffisante. Si $mp = m'p'$, supposons par l'absurde que $p \neq p'$, par exemple que $p' < p$. Comme p divise $m'p'$ en étant premier avec p', il divise m' d'après le Théorème de Gauss. Mais alors $p \leq m' < p'$, ce qui est absurde. Finalement $p = p'$ et $m = m'$.

B.IV.2.c. Posons $\mathcal{C} = \{(p,m) \in \mathcal{P} \times \mathbb{N}^* \,/\, m < p \leq x/m\}$. Il s'agit de montrer que l'application

$$\begin{array}{cccc} \Phi : & \mathcal{C} & \to & A(x) \\ & (p,m) & \mapsto & mp \end{array}$$

est une bijection. Φ est bien définie, et injective d'après la question précédente. Montrons qu'elle est surjective. Si $n \in A(x)$, il existe $m \in \mathbb{N}^*$ tel que

$$\left\{ \begin{array}{l} n = mp \text{ avec } p = P^+(n) > \sqrt{n} \\ 2 \leq n \leq x. \end{array} \right.$$

Dans ce cas $p = P^+(n)$ et $n \in A(x)$, et il suffit d'appliquer la question B.IV.2.a pour obtenir $m < p \leq x/m$. On a donc bien $(p,m) \in \mathcal{C}$ et $\Phi(p,m) = n$.

B.IV.2.d. Comme $\Phi : \mathcal{C} \to A(x)$ est bijective, $a(x) = |A(x)| = |\mathcal{C}|$. Si p est un nombre premier donné, combien existe-t-il d'entiers m tels que $(p,m) \in \mathcal{C}$? Autant que d'entiers $m \in \mathbb{N}^*$ tels que $m < p \leq x/m$, c'est-à-dire vérifiant

$$\left\{ \begin{array}{l} m \leq x/p \\ m < p. \end{array} \right.$$

Cela en fait $\text{Min}\left(p-1, \left[\frac{x}{p}\right]\right)$, et donc

$$|\mathcal{C}| = \sum_{p \in \mathcal{P}} \text{Min}\left(p-1, \left[\frac{x}{p}\right]\right).$$

Comme $\text{Min}\left(p-1, \left[\frac{x}{p}\right]\right) = 0$ dès que $p > x$, on a mieux :

$$|\mathcal{C}| = \sum_{p \leq x} \text{Min}\left(p-1, \left[\frac{x}{p}\right]\right).$$

B.IV.3.a. Comme $2p-1$ est toujours positif,

$$\begin{aligned} p \leq \varphi(x) &\Leftrightarrow 2p-1 \leq \sqrt{1+4x} \\ &\Leftrightarrow (2p-1)^2 \leq 1+4x \\ &\Leftrightarrow p^2 - p \leq x \quad \Leftrightarrow \quad p-1 \leq x/p \quad \Leftrightarrow \quad p-1 \leq [x/p]. \end{aligned}$$

B.IV.3.b. On a

$$\varphi(x) = \frac{1+\sqrt{1+4x}}{2} > \frac{\sqrt{4x}}{2} = \sqrt{x},$$

et

$$\begin{aligned}\varphi(x) < \sqrt{x}+1 &\Leftrightarrow 1+\sqrt{1+4x} < 2\sqrt{x}+2 \\ &\Leftrightarrow \sqrt{1+4x} < 2\sqrt{x}+1 \\ &\Leftrightarrow 1+4x < \left(2\sqrt{x}+1\right)^2 \quad \Leftrightarrow \quad 0 < 4\sqrt{x}\end{aligned}$$

donc l'assertion $\varphi(x) < \sqrt{x}+1$ est vraie.

B.IV.3.c. Les questions B.IV.2.d et B.IV.3.a donnent

$$\begin{aligned}a(x) &= \sum_{p\leq x} \mathrm{Min}\left(p-1, \left[\frac{x}{p}\right]\right) \\ &= \sum_{p\leq\varphi(x)} (p-1) + \sum_{\varphi(x)<p\leq x} \left[\frac{x}{p}\right]. \quad (\propto)\end{aligned}$$

$\sqrt{x}$ q φ(x) $\sqrt{x}+1$

FIG. 7.1 – Au plus un seul entier entre $\sqrt{x}$ et $\sqrt{x}+1$

• **Premier cas** : S'il n'existe pas de nombre premier dans $]\sqrt{x}, \varphi(x)]$, on obtient

$$a(x) = \sum_{p\leq\sqrt{x}} (p-1) + \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right]$$

comme désiré.

• **Deuxième cas** : S'il existe un nombre premier dans l'intervalle $]\sqrt{x}, \varphi(x)]$, celui-ci est unique (puisque $\sqrt{x} < \varphi(x) < \sqrt{x}+1$). Notons-le q. On est dans la situation de la FIG. 7.1, et $(\propto)$ s'écrit

$$\begin{aligned}a(x) &= \sum_{p\leq\sqrt{x}} (p-1) + (q-1) + \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] - \left[\frac{x}{q}\right] \\ &= \sum_{p\leq\sqrt{x}} (p-1) + \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] + T\end{aligned}$$

où $T = q - 1 - [x/q]$. Pour conclure, il faut démontrer que $T = 0$, ce que nous allons faire. De $\sqrt{x} < q < \sqrt{x} + 1$ on tire

$$\sqrt{x} - 1 < q - 1 < \sqrt{x}$$

et

$$\sqrt{x} - 1 < \frac{x}{\sqrt{x}+1} < \frac{x}{q} < \frac{x}{\sqrt{x}} = \sqrt{x}.$$

Comme $q \leq \varphi(x)$, B.IV.3.a montre que $q - 1 \leq [x/q]$, donc

$$\sqrt{x} - 1 < q - 1 \leq \left[\frac{x}{q}\right] < \sqrt{x}.$$

Les nombres $q - 1$ et $[x/q]$ sont entiers et appartiennent tous les deux à l'intervalle $]\sqrt{x} - 1, \sqrt{x}[$. Ils sont forcément égaux, donc $q - 1 = [x/q]$ et $T = 0$.

B.IV.3.d. On a

$$\sum_{p \leq \sqrt{x}} (p-1) \leq \sum_{p \leq \sqrt{x}} \sqrt{x} = \sqrt{x}\,\pi(\sqrt{x}).$$

La question A.II.3 montre que $\pi(\sqrt{x}) \leq e\sqrt{x}/\ln\sqrt{x}$ dès que x est suffisamment grand (voir Lemme 1), et dans ce cas

$$0 \leq \sum_{p \leq \sqrt{x}} (p-1) \leq 2e\frac{x}{\ln x}.$$

Comme $\frac{x}{\ln x} = o\,(x)$, cet encadrement montre que $\sum_{p \leq \sqrt{x}} (p-1) = o\,(x)$.

On a utilisé le résultat suivant :

Lemme 1 : Pour tout réel $x \geq 3$,

$$0 \leq \pi(x) \leq e\frac{x}{\ln x}$$

et en particulier $\pi(x) = o\,(x)$.

Preuve du Lemme 1 : La question A.II.3 montre que $0 \leq \pi(x) \leq e\frac{n}{\ln n}$ pour tout entier $n \geq 3$, donc

$$0 \leq \pi(x) = \pi([x]) \leq e\frac{[x]}{\ln [x]} \leq e\frac{x}{\ln x}$$

en utilisant la croissance de la fonction $x \mapsto \frac{x}{\ln x}$ sur $[e, +\infty[$. Ainsi

$$0 \leq \frac{\pi(x)}{x} \leq \frac{e}{\ln x}$$

avec $\lim_{x\to+\infty} \frac{e}{\ln x} = 0$, et on obtient $\lim_{x\to+\infty} \frac{\pi(x)}{x} = 0$ en appliquant le Théorème des gendarmes. Cela signifie que $\pi(x) = o\,(x)$. ■

B.IV.3.e. • On aura besoin du résultat suivant :

Lemme 2 : Pour tout réel $x \geq 3$,

$$\sum_{\sqrt{x}<p\leq x} \frac{1}{p} = \ln 2 + o\,(1)\,.$$

Preuve du Lemme 2 : Le résultat est assuré si $x = n$ est un entier naturel (question B.IV.1). Si x est réel,

$$A_x \leq \sum_{\sqrt{x}<p\leq x} \frac{1}{p} \leq B_x$$

avec

$$A_x = \sum_{\sqrt{x}<p\leq [x]} \frac{1}{p} = \sum_{\sqrt{[x]}<p\leq [x]} \frac{1}{p} - \sum_{\sqrt{[x]}<p\leq \sqrt{x}} \frac{1}{p}$$

et

$$B_x = \sum_{\sqrt{x}<p\leq [x]+1} \frac{1}{p} = \sum_{\sqrt{x}<p\leq \sqrt{[x]+1}} \frac{1}{p} + \sum_{\sqrt{[x]+1}<p\leq [x]+1} \frac{1}{p}.$$

Comme $\sqrt{[x]} < p \leq \sqrt{x}$ équivaut à $[x] < p^2 \leq x$ et comme aucun entier n'appartient à l'intervalle $][x], x]$, on a $\sum_{\sqrt{[x]}<p\leq\sqrt{x}} \frac{1}{p} = 0$ et

$$A_x = \sum_{\sqrt{[x]}<p\leq [x]} \frac{1}{p}$$

tend vers $\ln 2$ quand x tend vers $+\infty$ (d'après B.IV.1). Comme

$$\sqrt{x} < p \leq \sqrt{[x]+1} \quad \Leftrightarrow \quad x < p^2 \leq [x]+1,$$

le seul entier p qui pourrait être compris entre $\sqrt{x}$ et $\sqrt{[x]+1}$ est $\sqrt{[x]+1}$. On peut toujours écrire :

$$B_x \leq C_x = \frac{1}{\sqrt{[x]+1}} + \sum_{\sqrt{[x]+1}<p\leq [x]+1} \frac{1}{p}$$

et B.IV.1 montre que $\lim_{x\to+\infty} C_x = \ln 2$. Finalement

$$A_x \leq \sum_{\sqrt{x}<p\leq x} \frac{1}{p} \leq C_x$$

avec $\lim_{x\to+\infty} A_x = \lim_{x\to+\infty} C_x = \ln 2$, et le Théorème des gendarmes donne $\lim_{x\to+\infty} \sum_{\sqrt{x}<p\leq x} \frac{1}{p} = \ln 2$. ■

• Ce résultat étant acquis, on a

$$\sum_{\sqrt{x}<p\leq x} \left(\frac{x}{p}-1\right) \leq \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] \leq x \sum_{\sqrt{x}<p\leq x} \frac{1}{p}$$

soit

$$x \sum_{\sqrt{x}<p\leq x} \frac{1}{p} - \left(\pi(x) - \pi(\sqrt{x})\right) \leq \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] \leq x \sum_{\sqrt{x}<p\leq x} \frac{1}{p}.$$

En utilisant le Lemme 2, on obtient

$$x\ln 2 + o(x) - \pi(x) + \pi(\sqrt{x}) \leq \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] \leq x\ln 2 + o(x).$$

D'après le Lemme 1, $\pi(x) = o(x)$ et $\pi(\sqrt{x}) = o(\sqrt{x}) = o(x)$, donc

$$x\ln 2 + o(x) \leq \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] \leq x\ln 2 + o(x)$$

autrement dit

$$o(x) \leq \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] - x\ln 2 \leq o(x),$$

et cela montre que

$$\sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] = x\ln 2 + o(x).$$

B.IV.3.f. En conclusion

$$\begin{aligned} a(x) &= \sum_{p\leq\sqrt{x}} (p-1) + \sum_{\sqrt{x}<p\leq x} \left[\frac{x}{p}\right] \\ &= o(x) + (x\ln 2 + o(x)) \\ &= x\ln 2 + o(x), \end{aligned}$$

et

$$\lim_{x\to+\infty} \frac{a(x)}{x} = \lim_{x\to+\infty} (\ln 2 + o(1)) = \ln 2.$$

La densité de A est bien égale à $\ln 2 \simeq 0.69$, comme escompté.

Chapitre 8

Agrégation interne 2008, épreuve 1

8.1 Énoncé

Notations

On désigne par $\mathbb{C}$ le corps des nombres complexes.

Soit E un $\mathbb{C}$-espace vectoriel de dimension finie. On désigne par E^* l'espace vectoriel dual de E. On désigne par $\mathrm{End}(E)$ l'algèbre des endomorphismes de E et par $\mathrm{GL}(E)$ le groupe des endomorphismes inversibles de E. On note $\mathbf{1}_E$ l'application identique de E.

Si u est un endomorphisme de E, on note ${}^t u$ l'endomorphisme de E^* transposé de u ; si X est une partie de $\mathrm{End}(E)$, on note ${}^t X$ l'ensemble des transposés des éléments de X.

Soit u une application linéaire d'un espace vectoriel E dans un espace vectoriel E et soit x un vecteur de E. Pour alléger les notations, il nous arrivera d'écrire ux pour désigner l'image $u(x)$ du vecteur x par l'application u.

Soit n un entier ≥ 1 ; on désigne par $M_n(\mathbb{C})$ l'algèbre des matrices carrées complexes à n lignes et n colonnes. On note $E_{i,j}$ la matrice de $M_n(\mathbb{C})$ dont tous les coefficients sont nuls excepté celui de la i-ème ligne et j-ème colonne qui est égal à 1. On note $\mathrm{GL}(n,\mathbb{C})$ le groupe des matrices inversibles et $\mathbf{1}_n$ la matrice unité de $M_n(\mathbb{C})$.

Soient $\mathcal{A}$ et $\mathcal{B}$ deux $\mathbb{C}$-algèbres possédant chacune un élément unité ; un *morphisme unitaire* d'algèbres de $\mathcal{A}$ dans $\mathcal{B}$ est une application $\mathbb{C}$-linéaire qui préserve les produits et les éléments unités.

Les deux premières parties sont indépendantes. La sixième partie est indépendante des précédentes.

Partie I

1) Soit W un $\mathbb{C}$-espace vectoriel de dimension finie. Soient p_1, ..., p_n des endomorphismes de W. Pour $i = 1$, ..., n, on note W_i l'image de p_i. Démontrer que les conditions suivantes sont équivalentes :

(i) L'espace vectoriel W est somme directe des sous-espaces W_i et, pour $i = 1$, ..., n, p_i est le projecteur d'image W_i parallèlement à la somme directe des W_j, $j \neq i$.

(ii) Pour $i = 1$, ..., n, on a $p_i^2 = p_i$; pour $j \neq i$, on a $p_i p_j = 0$; et on a $p_1 + ... + p_n = \mathbf{1}_W$.

2) Soit toujours W un $\mathbb{C}$-espace vectoriel de dimension finie, soit n un entier ≥ 1 et soit $\rho : M_n(\mathbb{C}) \to \mathrm{End}(W)$ un morphisme unitaire d'algèbres.

a) Pour $i = 1$, ..., n, on note p_i l'endomorphisme $\rho(E_{i,i})$. Démontrer que les endomorphismes p_i satisfont à la condition (ii) de la question (I.1).

b) Pour $i = 1$, ..., n, on note W_i l'image de p_i. Démontrer que la restriction de $\rho(E_{i,j})$ à W_j induit un isomorphisme de W_j sur W_i.

c) Dans la suite de cette question, ou fixe une base $(w_1, ..., w_r)$ de l'espace vectoriel W_1. On pose

$$v_1 = w_1, \quad v_2 = \rho(E_{2,1})w_1, \ \dots , \quad v_n = \rho(E_{n,1})w_1.$$

Démontrer que la famille $(v_1, ..., v_n)$ est libre et que, pour tous entiers s, t et k compris entre 1 et n, on a

$$\rho(E_{s,t})v_k = \delta_{t,k} v_s,$$

où le symbole de Kronecker $\delta_{t,k}$ vaut 1 lorsque $t = k$, et vaut 0 sinon.

d) Plus généralement, pour $1 \leq j \leq r$, on note V_j le sous-espace vectoriel de W engendré par les vecteurs $\rho(E_{k,1})w_j$, pour $k = 1, ..., n$.
Démontrer que W est somme directe des sous-espaces V_j, $1 \leq j \leq r$.

e) Démontrer qu'il existe une base de l'espace vectoriel W dans laquelle, pour toute matrice $M \in M_n(\mathbb{C})$, la matrice de l'endomorphisme $\rho(M)$ est la matrice diagonale par blocs

$$\mathrm{diag}(M, ..., M) = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{pmatrix}.$$

Partie II

Dans cette partie, on désigne par E un $\mathbb{C}$-espace vectoriel de dimension finie. On dit qu'une partie X de $\mathrm{End}\,(E)$ est *irréductible* si les seuls sous-espaces vectoriels de E stables par tous les éléments de X sont $\{0\}$ et E. On désigne par $\mathcal{A}$ une sous-algèbre irréductible de $\mathrm{End}\,(E)$ qui contient $\mathbf{1}_E$, et on se propose de démontrer qu'elle est égale à $\mathrm{End}\,(E)$.

1) Soient u et v des éléments de $\mathrm{End}\,(E)$ qui commutent entre eux. Démontrer que tout sous-espace propre de l'un est stable par l'autre.

2) Soit X une partie irréductible de $\mathrm{End}\,(E)$. Démontrer que l'ensemble des endomorphismes de E qui commutent à tous les éléments de X est l'ensemble des endomorphismes scalaires.

3) Rappelons que $\mathcal{A}$ est une sous-algèbre irréductible de $\mathrm{End}\,(E)$ contenant $\mathbf{1}_E$. Démontrer que ${}^t\mathcal{A}$ est une sous-algèbre irréductible de $\mathrm{End}\,(E^*)$.

4) Soit x un vecteur non nul de E. Préciser à quoi est égal le sous-espace vectoriel $\mathcal{A}x$ de E.

5) Soit $u \in \mathrm{End}\,(E)$ un endomorphisme de rang 1. Démontrer qu'il existe un vecteur y de E et une forme linéaire $l \in E^*$ tels que l'on ait $u(x) = l\,(x)\,y$ pour tout $x \in E$.

6) Démontrer que, si l'algèbre $\mathcal{A}$ contient un endomorphisme de rang 1, alors elle les contient tous. En déduire que l'on a alors $\mathcal{A} = \mathrm{End}\,(E)$.

7) Dans cette question, on suppose que $\mathcal{A}$ contient un endomorphisme u dont le rang r est ≥ 2, et on se propose de démontrer qu'il existe un endomorphisme $u' \in \mathcal{A}$, non nul, dont le rang est strictement plus petit que r.

a) Démontrer qu'il existe x et y dans E et v dans $\mathcal{A}$ tels que le couple de vecteurs $(u\,(x)\,, u\,(y))$ soit libre et que l'on ait $vu\,(x) = y$.

b) Démontrer qu'il existe alors $\lambda \in \mathbb{C}$ tel que la restriction de l'endomorphisme $uv - \lambda \mathbf{1}_E$ à l'image $u\,(E)$ de u ne soit ni injective ni nulle.

c) Vérifier que l'endomorphisme $u' = uvu - \lambda u$ convient.

8) Démontrer finalement que $\mathcal{A} = \mathrm{End}\,(E)$.

Partie III

Soit n un entier ≥ 1. On appelle dérivation de $M_n\,(\mathbb{C})$ toute application linéaire d de $M_n\,(\mathbb{C})$ dans $M_n\,(\mathbb{C})$ telle que, pour tous X et $Y \in M_n\,(\mathbb{C})$, on ait

$$d\,(XY) = d\,(X)\,Y + X d\,(Y)\,.$$

1) Soit $A \in M_n(\mathbb{C})$; démontrer que l'application d_A de $M_n(\mathbb{C})$ dans $M_n(\mathbb{C})$ définie par $d_A(X) = AX - XA$ est une dérivation.

2) Dans cette question, on se propose de démontrer que toute dérivation de $M_n(\mathbb{C})$ est de la forme ci-dessus.

a) Soit $d : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ une dérivation. Démontrer que l'application ρ de $M_n(\mathbb{C})$ dans $M_{2n}(\mathbb{C})$ définie par

$$\rho(X) = \begin{pmatrix} X & d(X) \\ 0 & X \end{pmatrix}$$

est un morphisme unitaire d'algèbres.

b) Démontrer qu'il existe une matrice inversible $P = \begin{pmatrix} A & B \\ C & D \end{pmatrix}$ où A, B, C, D appartiennent à $M_n(\mathbb{C})$, telle que l'on ait, pour tout $X \in M_n(\mathbb{C})$,

$$P\,\rho(X) = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} P.$$

c) Conclure.

Partie IV

Soit n un entier ≥ 1. Pour toute matrice $M \in M_n(\mathbb{C})$, on note $\mathrm{Tr}(M)$ la trace de M, somme des coefficients diagonaux de M.

1) a) Démontrer que l'application ψ de $M_n(\mathbb{C}) \times M_n(\mathbb{C})$ dans $\mathbb{C}$ définie par

$$\psi(X, Y) = \mathrm{Tr}(XY),$$

est une forme bilinéaire symétrique non dégénérée.

b) Démontrer que, si $(X_1, ..., X_{n^2})$ est une base de l'espace vectoriel $M_n(\mathbb{C})$, il existe une autre base $(X'_1, ..., X'_{n^2})$ de $M_n(\mathbb{C})$ telle que, pour tous entiers i et j compris entre 1 et n^2, on ait

$$\psi(X_i, X'_j) = \delta_{i,j} \quad \text{(symbole de Kronecker).}$$

2) Démontrer que, pour toute matrice $A \in M_n(\mathbb{C})$, on a

$$\sum_{1 \leq i \leq n^2} X_i A X'_i = \mathrm{Tr}(A)\,\mathbf{1}_n.$$

Partie V

On considère dans cette partie un sous-groupe G de $\mathrm{GL}(n, \mathbb{C})$ ayant la propriété suivante :

(P) Il existe un entier $m \geq 1$ tel que l'on ait $g^m = \mathbf{1}_n$ pour tout $g \in G$.

On fixe l'entier m.

1) Démontrer que chaque élément g de G est diagonalisable. Que peut-on dire de ses valeurs propres ?

2) Démontrer que l'ensemble $\{\mathrm{Tr}(g),\ g \in G\}$ est fini.

3) On suppose, dans cette question, que l'ensemble G, considéré comme ensemble d'endomorphismes de $\mathbb{C}^n$ (en identifiant $M_n(\mathbb{C})$ et $\mathrm{End}(\mathbb{C}^n)$), est irréductible.

a) Démontrer que l'ensemble G contient une base de l'espace vectoriel $M_n(\mathbb{C})$.

b) Démontrer que l'ensemble G est fini (on pourra utiliser les questions (IV.1) et (V.2)).

4) Dans cette question, on ne suppose plus que l'ensemble G soit irréductible.

a) Démontrer qu'il existe des entiers p et q, avec $p + q = n$, et une base de l'espace vectoriel $\mathbb{C}^n$ dans laquelle chaque élément g de G s'écrit par blocs

$$\begin{pmatrix} T(g) & U(g) \\ 0 & V(g) \end{pmatrix}$$

où $T(g) \in M_p(\mathbb{C})$ et $V(g) \in M_q(\mathbb{C})$.

b) Posons $G_1 = \{g \in G \,/\, T(g) = \mathbf{1}_p\}$ et $G_2 = \{g \in G \,/\, V(g) = \mathbf{1}_q\}$. Démontrer que G_1 et G_2 sont des sous-groupes distingués de G. Déterminer $G_1 \cap G_2$.

c) Soient K un groupe et H un sous-groupe de K. L'indice de H dans K est le cardinal de l'ensemble quotient K/H. Etablir le résultat général suivant : Soient K un groupe, K_1 et K_2 des sous-groupes distingués de K, tous deux d'indice fini dans K ; alors l'indice de $K_1 \cap K_2$ dans K est fini.

d) Conclure.

Partie VI

Soient n et m des entiers ≥ 1. Soient $A \in M_n(\mathbb{C})$ et $B \in M_m(\mathbb{C})$; on

définit la matrice $A * B \in M_{nm}(\mathbb{C})$ par

$$A * B = \begin{pmatrix} a_{11}B & a_{12}B & \cdots & a_{1n}B \\ \vdots & \vdots & \cdots & \vdots \\ a_{n1}B & a_{n2}B & \cdots & a_{nn}B \end{pmatrix}.$$

1) Démontrer que l'application ϕ de $M_n(\mathbb{C}) \times M_m(\mathbb{C})$ dans $M_{nm}(\mathbb{C})$ définie par $\phi(A, B) = A * B$ est bilinéaire et satisfait à

$$(A * B)\left(A' * B'\right) = AA' * BB'$$

pour toutes matrices $A, A' \in M_n(\mathbb{C})$, $B, B' \in M_m(\mathbb{C})$.

2) Démontrer que l'image de l'application ϕ engendre l'espace vectoriel $M_{nm}(\mathbb{C})$.

On suppose désormais $n = m$.

3) Posons

$$P = \sum_{1 \leq i,j \leq n} E_{i,j} * E_{j,i}.$$

a) Démontrer que l'on a $P^2 = \mathbf{1}_{n^2}$.

b) Démontrer que, pour toutes matrices $A, B \in M_n(\mathbb{C})$, on a

$$P(A * B)P = B * A.$$

4) Soient A et $B \in M_n(\mathbb{C})$.

a) Calculer la trace et le déterminant de la matrice $A * B$.

b) Déterminer les valeurs propres de $A * B$ en fonction de celles de A et de B.

8.2 Corrigé

Partie I

I.1. ▶ (i) $\Rightarrow$ (ii) : Par hypothèse, tout vecteur x de W s'écrit de façon unique sous la forme $x = x_1 + ... + x_n$ où $x_i \in W_i$ quel que soit $i \in \{1, ..., n\}$. Par hypothèse aussi, p_i est la projection vectorielle sur W_i parallèlement à $\bigoplus_{j \neq i} W_j$, donc $p_i(x) = x_i$. On a donc

$$\forall x \in W \quad \mathbf{1}_W(x) = p_1(x) + ... + p_n(x),$$

c'est-à-dire $\mathbf{1}_W = p_1 + ... + p_n$.

Une projection étant un projecteur, on aura $p_i^2 = p_i$, ce qu'on peut vérifier en écrivant :

$$\forall x \in W \quad p_i^2 (x) = p_i (p_i (x)) = p_i (x_i) = x_i = p_i (x) .$$

Enfin, si $j \neq i$,

$$\forall x \in W \quad (p_i p_j) (x) = p_i (p_j (x)) = p_i (x_j) = 0$$

de par la définition même des projections p_i, donc $p_i p_j = 0$.

► (ii) ⇒ (i) : Pour tout $x \in W$,

$$x = \mathbf{1}_W (x) = p_1 (x) + ... + p_n (x) = x_1 + ... + x_n$$

en posant $p_i (x) = x_i$ pour tout i. Comme $x_i \in \mathrm{Im}(p_i) = W_i$, on en déduit que $W = W_1 + ... + W_n$. Montrons que cette décomposition de x en somme $x = x_1 + ... + x_n$ est unique, ce qui nous permettra d'affirmer que nous avons la somme directe

$$W = W_1 \oplus ... \oplus W_n . \quad (1)$$

Si $x = x_1 + ... + x_n = y_1 + ... + y_n$ avec $x_i, y_i \in W_i$ pour tout i, alors

$$p_i (x) = p_i (x_1) + ... + p_i (x_n) . \quad (2)$$

Si $j \neq i$, le vecteur x_j appartient à $W_j = \mathrm{Im}\, p_j$ donc s'écrit $x_j = p_j (z_j)$ pour un certain vecteur z_j de W. Mais alors $p_i (x_j) = (p_i p_j) (z_j) = 0$. En remplaçant dans (2), on obtient $p_i (x) = p_i (x_i)$. Mais $x_i \in W_i$, donc il existe $z_i \in W$ tel que $x_i = p_i (z_i)$, et

$$p_i (x) = p_i (x_i) = p_i^2 (z_i) = p_i (z_i) = x_i .$$

Il suffit de recommencer avec la décomposition $x = y_1 + ... + y_n$ pour obtenir $p_i (x) = y_i$ et conclure à

$$\forall i \in \{1, ..., n\} \quad x_i = p_i (x) = y_i .$$

L'unicité est prouvée, et l'égalité (1) est démontrée.

Le reste est facile, puisque dans la démonstration précédente, nous avons prouvé que tout vecteur x de W, qui s'écrit $x = x_1 + ... + x_n$ dans la somme directe $W = W_1 \oplus ... \oplus W_n$, est tel que $p_i (x) = x_i$ et $p_i (x_j) = 0$ si $j \neq i$. Par la définition même d'une projection, cela signifie que p_i est la projection sur W_i parallèlement à $\bigoplus_{j \neq i} W_j$.

I.2.a. Appliquer ρ aux deux membres de l'égalité $E_{i,i}^2 = E_{i,i}$ donne $p_i^2 = p_i$. De même, si $i \neq j$, $E_{i,i} \times E_{j,j} = 0$ entraîne $\rho (E_{i,i}) \times \rho (E_{j,j}) = \rho (0) = 0$, c'est-à-dire $p_i p_j = 0$. Enfin l'égalité $\mathbf{1}_n = E_{1,1} + ... + E_{n,n}$ entraîne $\mathbf{1}_W = p_1 + ... + p_n$.

I.2.b. ► J'ai besoin de savoir à quoi est égal le produit $E_{i,j} \times E_{u,v}$ (qu'on a déjà utilisé dans la question précédente !) :

Lemme E : Quels que soient les couples d'indices (i,j) et (u,v),

$$E_{i,j} \times E_{u,v} = \begin{cases} 0 & \text{si } j \neq u \\ E_{i,v} & \text{si } j = u, \end{cases}$$

ce qu'on peut résumer en écrivant : $E_{i,j} \times E_{u,v} = \delta_{j,u} E_{i,v}$.

Preuve : Posons $E_{i,j} = (a_{l,c}) = (\delta_{l,i}\delta_{c,j})$, $E_{u,v} = (b_{l,c}) = (\delta_{l,u}\delta_{c,v})$ et enfin $E_{i,j} \times E_{u,v} = (d_{l,c})$. On a

$$d_{l,c} = \sum_{k=1}^{n} a_{l,k} b_{k,c} = \sum_{k=1}^{n} \delta_{l,i}\delta_{k,j}\delta_{k,u}\delta_{c,v} = \begin{cases} 0 & \text{si } j \neq u \\ \delta_{l,i}\delta_{c,v} & \text{si } j = u, \end{cases}$$

donc $E_{i,j} \times E_{u,v} = (\delta_{l,i}\delta_{c,v}) = E_{i,v}$ si $j = u$, et $E_{i,j} \times E_{u,v} = 0$ sinon. ■

▶ Pour tout $x \in W$,

$$\rho(E_{i,j})\,(x) = \rho(E_{i,i}E_{i,j})\,(x) = \rho(E_{i,i})\,[\rho(E_{i,j})\,(x)] \in \operatorname{Im}\rho(E_{i,i}) = W_i,$$

donc $\operatorname{Im}\rho(E_{i,j}) \subset W_i$, et on peut parler de l'application

$$\rho(E_{i,j})|_{W_j} : W_j \to W_i.$$

On notera que $\rho(E_{i,j})|_{W_j}$ est ici obtenue par restriction au départ et à l'arrivée (ce qui n'est pas la définition usuelle d'une restriction).

▶ Posons

$$f_{i,j} = \rho(E_{i,j})|_{W_j} : W_j \to W_i \quad \text{et} \quad f_{j,i} = \rho(E_{j,i})|_{W_i} : W_i \to W_j.$$

$f_{i,j}$ et $f_{j,i}$ sont linéaires, et

$$f_{j,i} \circ f_{i,j} = (\rho(E_{j,i}) \circ \rho(E_{i,j}))\,|_{W_j} = \rho(E_{j,i}E_{i,j})|_{W_j} = \rho(E_{j,j})|_{W_j} = \mathbf{1}_{W_j}$$

puisque $p_j = \rho(E_{j,j})$ est la projection sur W_j parallèlement à $\bigoplus_{k \neq j} W_k$, donc admet W_j comme sous-espace vectoriel des vecteurs invariants. On obtiendrait de même : $f_{i,j} \circ f_{j,i} = \mathbf{1}_{W_i}$. Ainsi $f_{j,i} \circ f_{i,j} = \mathbf{1}_{W_j}$ et $f_{i,j} \circ f_{j,i} = \mathbf{1}_{W_i}$, et $f_{i,j}$ est un isomorphisme W_j sur W_i, de fonction réciproque $f_{j,i}$.

Autre solution : Il est tout à fait possible de montrer que l'application linéaire $f_{i,j} = \rho(E_{i,j})|_{W_j} : W_j \to W_i$ est un isomorphisme en vérifiant qu'elle est injective et surjective. L'injectivité se vérifie en montrant que le noyau

$$\operatorname{Ker} f_{i,j} = W_j \cap \{x \in W \,/\, \rho(E_{i,j})\,(x) = 0\}$$

est réduit au singleton $\{0\}$. C'est trivial si $i = j$, puisqu'alors $f_{i,i} = p_i|_{W_i} = \mathbf{1}_{W_i}$ est injective ! Dans le cas où $i \neq j$, on note que

$$x \in \operatorname{Ker} f_{i,j} \;\Leftrightarrow \left\{ \begin{array}{l} x \in W_j \\ \rho(E_{i,j})\,(x) = 0 \end{array} \right. \;\Leftrightarrow\; \left\{ \begin{array}{l} \exists z \in W \quad x = \rho(E_{j,j})\,(z) \\ \rho(E_{i,j})\,(x) = 0. \end{array} \right.$$

Avec ces notations, si $x \in \operatorname{Ker} f_{i,j}$, on obtient $\rho(E_{i,j})\,(\rho(E_{j,j})\,(z)) = 0$, donc $\rho(E_{i,j}E_{j,j})\,(z) = 0$, soit $\rho(E_{i,j})\,(z) = 0$. Par suite

$$x = \rho(E_{j,j})\,(z) = \rho(E_{j,i}E_{i,j})\,(z) = \rho(E_{j,i})\,(\rho(E_{i,j})\,(z)) = \rho(E_{j,i})\,(0) = 0.$$

On vient de prouver l'implication

$$x \in \operatorname{Ker} f_{i,j} \quad \Rightarrow \quad x = 0$$

autrement dit que $\operatorname{Ker} f_{i,j} = \{0\}$.
Montrons maintenant que $f_{i,j}$ est surjective. Si $y \in W_i$, il existe $x \in W$ tel que $y = \rho(E_{i,i})\,(x)$. Par suite

$$y = \rho(E_{i,i})\,(x) = \rho(E_{i,j}E_{j,i})\,(x) = \rho(E_{i,j})\,(\rho(E_{j,i})\,(x)) \in \operatorname{Im} \rho(E_{i,j})$$

où $\rho(E_{j,i})\,(x)$ appartient à W_j puisque

$$\rho(E_{j,i})\,(x) = \rho(E_{j,j})\,(\rho(E_{j,i})\,(x)) \in \operatorname{Im} \rho(E_{j,j}) = W_j.$$

Ainsi $y \in \operatorname{Im} \rho(E_{i,j})|_{W_j} = \operatorname{Im} f_{i,j}$. On a bien montré l'inclusion $W_i \subset \operatorname{Im} f_{i,j}$.

I.2.c. ► Si $(\alpha_1, ..., \alpha_n) \in \mathbb{C}^n$ vérifie $\alpha_1 v_1 + \alpha_2 v_2 + ... + \alpha_n v_n = 0$, alors

$$\underbrace{\alpha_1 w_1}_{\in W_1} + \underbrace{\alpha_2 \rho(E_{2,1}) w_1}_{\in W_2} + ... + \underbrace{\alpha_n \rho(E_{n,1}) w_1}_{\in W_n} = 0.$$

Comme $W = W_1 \oplus ... \oplus W_n$, cela entraîne

$$\alpha_1 w_1 = \alpha_2 \rho(E_{2,1}) w_1 = ... = \alpha_n \rho(E_{n,1}) w_1 = 0.$$

Il suffit de rappeler que $w_1 \neq 0$ et que $\rho(E_{k,1})$ induit un isomorphisme de W_1 sur W_k, donc transforme le vecteur non nul w_1 en un vecteur non nul $\rho(E_{k,1})w_1$, pour en déduire $\alpha_1 = \alpha_2 = ... = \alpha_n = 0$. Cela montre que la famille $(v_1, ..., v_n)$ est libre.

► Soient $s, t, k \in \{1, ..., n\}$. Le Lemme E permet d'écrire

$$\begin{aligned} \rho(E_{s,t}) v_k &= \rho(E_{s,t}) \rho(E_{k,1}) w_1 \\ &= \rho(E_{s,t} E_{k,1}) w_1 \\ &= \rho(\delta_{t,k} E_{s,1}) w_1 = \delta_{t,k} \rho(E_{s,1}) w_1 = \delta_{t,k} v_s. \end{aligned}$$

I.2.d. • **Première solution :** On sait que $W = W_1 \oplus ... \oplus W_n$ et que W_k admet la base $(\rho(E_{k,1})w_1, ..., \rho(E_{k,1})w_r)$ puisque $\rho(E_{k,1})|_{W_1} : W_1 \to W_k$ est un isomorphisme. Donc tout élément x de W s'écrit de façon unique sous la forme $x = x_1 + ...x_n$, avec $x_k \in W_k$, et pour k fixé, tout x_k s'écrit de façon unique sous la forme

$$x_k = \alpha_{k,1}\rho(E_{k,1})w_1 + ... + \alpha_{k,r}\rho(E_{k,1})w_r$$

avec $(\alpha_{k,1}, ..., \alpha_{k,r}) \in \mathbb{C}^r$. On peut donc affirmer que tout $x \in W$ s'écrit de façon unique sous la forme

$$x = \sum_{\substack{1\leq k\leq n \\ 1\leq j\leq r}} \alpha_{k,j}\rho(E_{k,1})w_j.$$

Cela prouve que la famille $(\rho(E_{k,1})w_j)_{1\leq k\leq n, 1\leq j\leq r}$ est une base de W. Comme

$$V_j = \mathrm{Vect}\{\rho(E_{k,1})w_j \,/\, k = 1, ..., n\},$$

on en déduit que $W = V_1 \oplus ... \oplus V_r$.

• **Deuxième solution :** En raisonnant comme dans la question précédente, on montre que $(\rho(E_{k,1})w_j)_{1\leq k\leq n}$ est une base de V_j. Montrer que $W = V_1 \oplus ... \oplus V_r$ revient à prouver que $\mathcal{B} = (\rho(E_{k,1})w_j)_{1\leq k\leq n, 1\leq j\leq r}$ est une base de W. Or $W = W_1 \oplus ... \oplus W_n$ (I.2.a) et le sous-espace W_j est toujours isomorphe à W_1 (I.2.b), donc

$$\dim W = r \dim W_1 = nr.$$

Comme $\mathcal{B}$ est une famille de nr vecteurs, montrer qu'il s'agit d'une base de W revient à montrer que $\mathcal{B}$ est libre. Pour ce faire, considérons une combinaison linéaire nulle de ces vecteurs :

$$\sum_{k,j} \alpha_{k,j}\rho(E_{k,1})w_j = 0.$$

En appliquant $\rho(E_{1,k'})$, on trouve

$$\sum_{k,j} \alpha_{k,j}\rho(E_{1,k'}E_{k,1})w_j = 0.$$

Comme $E_{1,k'}E_{k,1} = 0$ si $k \neq k'$, et $\rho(E_{1,k}E_{k,1})w_j = \rho(E_{1,1})w_j = w_j$ (d'après le Lemme E et puisque $\rho(E_{1,1})$ est une projection sur W_1), on obtient

$$\sum_{j} \alpha_{k',j}w_j = 0,$$

ce qui entraîne $\alpha_{k',1} = ... = \alpha_{k',r} = 0$ puisque $(w_1..., w_r)$ est une base de W_1. Cela achève la démonstration.

I.2.e. On considère la base $\mathcal{B} = (\rho(E_{k,1})w_j)_{1\leq k\leq n, 1\leq j\leq r}$ de W obtenue à la question précédente. Cette base est adaptée à la somme directe

$$W = V_1 \oplus ... \oplus V_r,$$

puisqu'elle est formée de la juxtaposition des bases $\mathcal{B}_j = (\rho(E_{k,1})w_j)_{1\leq k\leq n}$ des V_j. On doit vérifier que, pour tout $M \in M_n(\mathbb{C})$, la matrice $\operatorname{Mat}(\rho(M); \mathcal{B})$ de $\rho(M)$ dans la base $\mathcal{B}$ est de la forme

$$\operatorname{Mat}(\rho(M); \mathcal{B}) = \begin{pmatrix} \overbrace{M}^{V_1} & 0 & \cdots & \overbrace{0}^{V_j} & \cdots & \overbrace{0}^{V_r} \\ 0 & M & \cdots & \vdots & \cdots & 0 \\ \vdots & & & \vdots & & \vdots \\ & & & M & & \vdots \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & \cdots & M \end{pmatrix}$$

où les colonnes regroupées sous l'appellation V_j sont formées des coordonnées des vecteurs de la base $\mathcal{B}_j$ de V_j dans la base $\mathcal{B}$. Si $m_{u,v}$ désignent les coefficients de M,

$$M = (m_{u,v}) = \sum_{1\leq u,v\leq n} m_{u,v} E_{u,v}$$

et

$$\rho(M)\left(\rho(E_{k,1})w_j\right) = \sum_{u,v} m_{u,v}\rho(E_{u,v})\rho(E_{k,1})w_j = \sum_{u} m_{u,k}\rho(E_{u,k})\rho(E_{k,1})w_j$$

puisque $\rho(E_{u,v})\rho(E_{k,1}) = \rho(E_{u,v}E_{k,1}) = \rho(0) = 0$ si $v \neq k$ (Lemme E). Comme

$$\rho(E_{u,k})\rho(E_{k,1})w_j = \rho(E_{u,k}E_{k,1})w_j = \rho(E_{u,1})w_j,$$

on obtient

$$\rho(M)\left(\rho(E_{k,1})w_j\right) = \sum_{u} m_{u,k}\rho(E_{u,1})w_j.$$

Cela montre que $\rho(M)$ transforme un vecteur de V_j en un vecteur de V_j, donc que $\rho(M)$ est une matrice formés de blocs de dimensions r situés sur la diagonale principale, et de 0 partout ailleurs. Mieux, on constate que la matrice

de la restriction $\rho(M)|_{V_j} : V_j \to V_j$ dans la base $\mathcal{B}_j$ est $M = (m_{u,k})_{1\leq u,k\leq n}$. Finalement, on obtient bien

$$\operatorname{Mat}(\rho(M);\mathcal{B}) = \begin{pmatrix} M & 0 & \cdots & 0 \\ 0 & M & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & M \end{pmatrix}.$$

Partie II

II.1. Notons $E_u(\lambda)$ le sous-espace propre de u associé à la valeur propre λ.

$$\forall x \in E_u(\lambda) \quad u(v(x)) = v(u(x)) = v(\lambda x) = \lambda v(x)$$

donc

$$\forall x \in E_u(\lambda) \quad v(x) \in E_u(\lambda).$$

Ainsi $v(E_u(\lambda)) \subset E_u(\lambda)$ et tout sous-espace propre de u est stable par v. On peut bien sûr inverser les rôles de u et v qui sont symétriques.

II.2. Si $u \in \operatorname{End}(E)$ commute avec tous les éléments de X, considérons une valeur propre λ de u (il en existe car le polynôme caractéristique de u possède toujours au moins une racine dans $\mathbb{C}$, qui est algébriquement clos) et notons toujours $E_u(\lambda)$ le sous-espace propre de u associé à λ.
Tout élément v de X commute avec u, donc laisse stable $E_u(\lambda)$ d'après la question précédente. Comme X est irréductible, on en déduit

$$E_u(\lambda) = \{0\} \text{ ou } E.$$

Mais $E_u(\lambda) \neq \{0\}$ puisqu'un espace propre n'est jamais réduit à $\{0\}$! Donc $E_u(\lambda) = E$, et u est l'homothétie vectorielle de rapport λ.

II.3. • *Montrons que* ${}^t\mathcal{A} = \left\{ {}^tu \,/\, u \in \mathcal{A} \right\}$ *est une sous-algèbre de* $\operatorname{End}(E^*)$.
Il s'agit de montrer les trois points suivants[1] :

a) ${}^t\mathcal{A}$ n'est pas vide, car contient ${}^t\mathbf{1}_E$.

[1] Rappelons qu'un ensemble A muni de deux lois internes "+" et "$\circ$", et d'une loi externe "." de $K \times A$ dans A, est une algèbre sur un corps K si a) $(A,+,.)$ est un espace vectoriel sur K ; b) $(A,+,\circ)$ est un anneau ; c) Les multiplications externe "." et interne "$\circ$" vérifient la relation de compatibilité $\lambda(f\circ g) = (\lambda f)\circ g = f \circ (\lambda g)$ pour tous $\lambda \in K$ et $f, g \in A$. La caractérisation d'une sous-algèbre que l'on utilise ici est obtenue à partir de cette définition, en utilisant les caractérisations classiques des sous-espaces vectoriels et des sous-anneaux.

b) Pour tous ${}^t u$, ${}^t v \in {}^t\mathcal{A}$ (avec $u, v \in \mathcal{A}$) et tout $\lambda \in \mathbb{C}$, ${}^t u + \lambda\, {}^t v \in {}^t\mathcal{A}$. C'est trivial puisque

$${}^t u + \lambda\, {}^t v = {}^t (u + \lambda v)$$

et que $u + \lambda v \in \mathcal{A}$ (puisque $\mathcal{A}$ est une algèbre).

c) Pour tous ${}^t u$, ${}^t v \in {}^t\mathcal{A}$ (avec $u, v \in \mathcal{A}$), ${}^t u \circ {}^t v \in {}^t\mathcal{A}$. C'est évident car

$${}^t u \circ {}^t v = {}^t (v \circ u)$$

et $v \circ u \in \mathcal{A}$, puisque $\mathcal{A}$ est une algèbre.

- *Montrons que ${}^t\mathcal{A}$ est irréductible.*

Si V est un sous-espace de E^* stable par tous les éléments de ${}^t\mathcal{A}$, le Lemme S démontré plus loin prouve que l'orthogonal V^o de V dans E est stable par tous les éléments de $\mathcal{A}$.
Comme $\mathcal{A}$ est irréductible, on en déduit que $V^o = \{0\}$ ou E, d'où[2]

$$V = (V^o)^\perp = \{0\}^\perp \text{ ou } E^\perp = E^* \text{ ou } \{0\},$$

où le symbole $^\perp$ signifie que l'on prend l'orthogonal d'une partie de E dans E^*. Les seuls sous-espaces stables par tous les éléments de ${}^t\mathcal{A}$ sont donc E^* et $\{0\}$, et ${}^t\mathcal{A}$ est bien irréductible.

Lemme S : Soient V un sous-espace vectoriel de E^*, et V^o son orthogonal dans E. Alors

$$\left(\begin{array}{l} V \text{ stable par tous} \\ \text{les éléments de } {}^t\mathcal{A} \end{array} \right) \Rightarrow \left(\begin{array}{l} V^o \text{ stable par tous} \\ \text{les éléments de } \mathcal{A} \end{array} \right).$$

Preuve : Pour tout $v \in \mathcal{A}$, pour tout $x \in V^o$ et tout $u \in V$,

$$< u, v(x) > = < {}^t v\,(u)\,, x > = 0$$

puisque ${}^t v\,(u) \in V$ par hypothèse. Cela prouve que $v(V^o) \subset V^o$, autrement dit que V^o est stable par v. ■

II.4. $\mathcal{A}x = \{v\,(x) \;/\; v \in \mathcal{A}\}$ est un sous-espace vectoriel de E stable par $\mathcal{A}$ et non réduit à $\{0\}$ puisque contenant $\mathbf{1}_E\,(x) = x$ qui n'est pas nul. Comme $\mathcal{A}$ est irréductible, on aura $\mathcal{A}x = E$.

---

[2] La formule $V = (V^o)^\perp$ est une formule de cours, vraie quand les espaces sont de dimension finie. On pourra se reporter à la Section 9.3 de [22] qui traite de tout ce qu'il faut connaître sur la dualité.

II.5. Par hypothèse, $\operatorname{Im} u$ est une droite vectorielle. Si y est un vecteur non nul de $\operatorname{Im} u$, on a donc $\operatorname{Im} u = \mathbb{C}y$, et pour tout $x \in E$ il existe $k_x \in \mathbb{C}$ tel que $u(x) = k_x y$. Pour conclure, il suffit de vérifier que l'application

$$l : \begin{array}{ccc} E & \to & \mathbb{C} \\ x & \mapsto & k_x \end{array}$$

est linéaire. Pour tout $(x, x') \in E^2$ et $\lambda \in \mathbb{C}$,

$$\left\{ \begin{array}{l} u(x + \lambda x') = k_{x+\lambda x'} y \\ u(x + \lambda x') = u(x) + \lambda u(x') = k_x y + \lambda k_{x'} y = (k_x + \lambda k_{x'}) y \end{array} \right.$$

donc $k_{x+\lambda x'} = k_x + \lambda k_{x'}$, et la linéarité de l s'en déduit.

II.6. • Supposons que $\mathcal{A}$ contienne un endomorphisme u de rang 1. La question précédente montre l'existence d'un vecteur y non nul et d'une forme linéaire l tels que

$$\forall x \in E \quad u(x) = l(x)\, y.$$

Soit v un endomorphisme quelconque de rang 1 de E. Il existe un vecteur non nul $z \in E$ et une forme linéaire h tels que

$$\forall x \in E \quad v(x) = h(x)\, z.$$

D'après II.4, $\mathcal{A}y = E$ donc il existe $w \in \mathcal{A}$ tel que $w(y) = z$. Par suite

$$\forall x \in E \quad (w \circ u)(x) = l(x)\, w(y) = l(x)\, z. \quad (*)$$

La question II.4 appliquée avec l'algèbre ${}^t\mathcal{A}$ et le vecteur $l \in E^*$ montre que ${}^t\mathcal{A}l = E^*$, de sorte qu'il existe $\xi \in \mathcal{A}$ tel que ${}^t\xi(l) = h$. Cela s'écrit encore (avec des crochets de dualité) :

$$\forall x \in E \quad < {}^t\xi(l), x > = < h, x > .$$

Comme $< {}^t\xi(l), x > = < l, \xi(x) > = l(\xi(x))$, on obtient

$$\forall x \in E \quad l(\xi(x)) = h(x)$$

ou encore $l \circ \xi = h$. En remplaçant x par $\xi(x)$ dans $(*)$, on trouve

$$\forall x \in E \quad (w \circ u)(\xi(x)) = l(\xi(x))\, z = h(x)\, z = v(x)$$

soit $v = w \circ u \circ \xi$. Finalement, v est la composée de trois applications de $\mathcal{A}$, donc appartient à $\mathcal{A}$.
En conclusion : tous les endomorphismes de rang 1 appartiennent à $\mathcal{A}$.

• Montrons que $\mathcal{A} = \text{End}(E)$.

L'inclusion $\mathcal{A} \subset \text{End}(E)$ est évidente. Réciproquement, si $u \in \text{End}(E)$, montrons que $u \in \mathcal{A}$. Choisissons une base $(e_1, ..., e_n)$ de E et écrivons tout vecteur x de E sous la forme $x = \sum_{i=1}^n x_i e_i$, où $x_1, ..., x_n \in \mathbb{C}$. Alors

$$\forall x \in E \qquad u(x) = u\left(\sum_{i=1}^n x_i e_i\right) = \sum_{i=1}^n x_i u(e_i).$$

Pour tout i, posons $u(e_i) = y_i$. On peut supposer u non nulle (sinon il n'y a rien à démontrer, l'application nulle étant de facto dans l'algèbre $\mathcal{A}$) et définir $I = \{i \in \{1, ..., n\} \,/\, y_i \neq 0\}$. Alors

$$\forall x \in E \quad u(x) = \sum_{i \in I} x_i y_i$$

et pour tout $i \in I$, l'application

$$u_i : \begin{array}{ccc} E & \to & E \\ x & \mapsto & x_i y_i \end{array}$$

est un endomorphisme de E de rang 1, donc appartient à $\mathcal{A}$. On a

$$\forall x \in E \quad u(x) = \sum_{i \in I} u_i(x)$$

donc $u = \sum_{i \in I} u_i$. L'endomorphisme u est ainsi combinaison linéaire d'éléments de $\mathcal{A}$, donc appartient à $\mathcal{A}$ (puisque $\mathcal{A}$ est un sous-espace vectoriel).

Remarque : Les applications u_i sont des endomorphismes de E comme on le voit facilement en introduisant la base $(e_1^*, ..., e_n^*)$ duale de $(e_1, ..., e_n)$, et en écrivant $u_i(x) = x_i y_i = e_i^*(x)\, y_i$. On a évidemment $\text{Im}\, u_i \subset \mathbb{C} y_i$. Pour montrer l'égalité $\text{Im}\, u_i = \mathbb{C} y_i$, on peut soit remarquer que $u_i(e_i) = y_i \neq 0$, et donc que le sous-espace $\text{Im}\, u_i$, non réduit à $\{0\}$, ne peut qu'être égal à $\mathbb{C} y_i$; soit se donner un vecteur quelconque λy_i de $\mathbb{C} y_i$, et noter que $\lambda y_i = u_i(\lambda e_i) \in \text{Im}\, u_i$.

II.7.a. Comme $\text{rg}(u) \geq 2$, il existe $x, y \in E$ tels que $(u(x), u(y))$ soit libre. Cela impose d'avoir $u(x) \neq 0$, el la question II.4 montre que $\mathcal{A}u(x) = E$. Il existe donc $v \in \mathcal{A}$ tel que $y = vu(x)$.

II.7.b. On a $uv(\text{Im}\, u) \subset \text{Im}\, u$, donc on peut considérer la restriction (au départ et à l'arrivée) :

$$uv|_{\text{Im}\, u} : \text{Im}\, u \to \text{Im}\, u.$$

Dire que $(uv - \lambda \mathbf{1}_E)\,|_{\text{Im}\, u}$ est injective revient à dire que λ n'est pas valeur propre de $uv|_{\text{Im}\, u}$. Je choisis donc une valeur propre complexe quelconque λ de $uv|_{\text{Im}\, u}$, et je suis certain que $(uv - \lambda \mathbf{1}_E)\,|_{\text{Im}\, u}$ ne sera pas injective.

Le calcul

$$(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u}(u(x)) = uvu(x) - \lambda u(x) = u(y) - \lambda u(x)$$

montre que $(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u}(u(x))$ n'est pas nul (sinon $(u(x), u(y))$ serait lié), donc que $(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u}$ n'est pas l'application nulle.

II.7.c. • Si u' était nul, on aurait

$$u'(x) = (uvu - \lambda u)(x) = u(y) - \lambda u(x) = 0$$

et $(u(x), u(y))$ serait lié, absurde. Donc u' n'est pas nul.

• L'image de $u' = (uv - \lambda \mathbf{1}_E) u$ est exactement celle de $(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u}$, et on sait que $(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u} : \operatorname{Im} u \to \operatorname{Im} u$ n'est pas injective. Donc

$$\operatorname{rg} u' = \operatorname{rg}(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u} = \dim(\operatorname{Im}(uv - \lambda \mathbf{1}_E)|_{\operatorname{Im} u}) < \dim \operatorname{Im} u = \operatorname{rg} u;$$

d'où $\operatorname{rg} u' < \operatorname{rg} u$.

II.8. Comme $\mathcal{A} \neq \{0\}$ ($\mathcal{A}$ contient $\mathbf{1}_E$), montrer que $\mathcal{A} = \operatorname{End}(E)$ revient à prouver que la propriété suivante est vraie quel que soit $k \in \mathbb{N}^*$:

$H(k)$: "S'il existe $u \in \mathcal{A}$ de rang $\leq k$, alors $\mathcal{A} = \operatorname{End}(E)$."

On raisonne par récurrence sur k. La propriété $H(1)$ a été démontrée en II.6. Si $H(k-1)$ est vraie, et si $u \in \mathcal{A}$ est de rang k, II.7 montre qu'il est possible de construire $u' \in \mathcal{A}$ tel que $\operatorname{rg} u' < \operatorname{rg} u = k$. On peut alors appliquer l'hypothèse récurrente au rang k et conclure à $\mathcal{A} = \operatorname{End}(E)$.

Partie III

III.1. L'application $d_A : M_n(\mathbb{C}) \to M_n(\mathbb{C})$ est linéaire, puisque pour tous $X,Y \in M_n(\mathbb{C})$ et tout $\lambda \in \mathbb{C}$,

$$\begin{aligned} d_A(X + \lambda Y) &= A(X + \lambda Y) - (X + \lambda Y) A \\ &= (AX - XA) + \lambda(AY - YA) \\ &= d_A(X) + \lambda d_A(Y), \end{aligned}$$

et telle que

$$\begin{aligned} d_A(XY) &= AXY - XYA \\ &= (AX - XA) Y + X(AY - YA) \\ &= d_A(X) Y + X d_A(Y) \end{aligned}$$

pour tous X, Y. C'est donc une dérivation.

III.2.a. On a

$$\rho(\mathbf{1}_n) = \begin{pmatrix} \mathbf{1}_n & d(\mathbf{1}_n) \\ 0 & \mathbf{1}_n \end{pmatrix} = \begin{pmatrix} \mathbf{1}_n & 0 \\ 0 & \mathbf{1}_n \end{pmatrix} = \mathbf{1}_{2n}.$$

Pour tous $X,Y \in M_n(\mathbb{C})$ et $\lambda \in \mathbb{C}$,

$$\begin{aligned}\rho(X+\lambda Y) &= \begin{pmatrix} X+\lambda Y & d(X+\lambda Y) \\ 0 & X+\lambda Y \end{pmatrix} \\ &= \begin{pmatrix} X & d(X) \\ 0 & X \end{pmatrix} + \lambda \begin{pmatrix} Y & d(Y) \\ 0 & Y \end{pmatrix} \\ &= \rho(X) + \lambda\rho(Y)\end{aligned}$$

puisque d est linéaire. Enfin

$$\begin{aligned}\rho(X)\rho(Y) &= \begin{pmatrix} X & d(X) \\ 0 & X \end{pmatrix}\begin{pmatrix} Y & d(Y) \\ 0 & Y \end{pmatrix} \\ &= \begin{pmatrix} XY & Xd(Y)+d(X)Y \\ 0 & XY \end{pmatrix} \\ &= \begin{pmatrix} XY & d(XY) \\ 0 & XY \end{pmatrix} = \rho(XY)\end{aligned}$$

pour tous X, Y. Cela prouve que ρ est un morphisme unitaire d'algèbres.

III.2.b. Posons $W = \mathbb{C}^{2n}$. W est un $\mathbb{C}$-espace vectoriel tel que l'espace $\mathrm{End}(W)$ soit isomorphe à $M_{2n}(\mathbb{C})$. On peut donc identifier $\mathrm{End}(W)$ et $M_{2n}(\mathbb{C})$ (moyennant le choix d'une base de W) et considérer

$$\rho : M_n(\mathbb{C}) \to \mathrm{End}(W) = M_{2n}(\mathbb{C})$$

comme un morphisme d'algèbres unitaires. La question I.2.e montre alors qu'il existe une base de W dans laquelle, pour toute $X \in M_n(\mathbb{C})$, la matrice de l'endomorphisme $\rho(X)$ soit de la forme :

$$\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}.$$

Cela revient à affirmer l'existence d'une matrice inversible $P \in M_{2n}(\mathbb{C})$ (une matrice de changement de bases) telle que

$$\forall X \in M_n(\mathbb{C}) \quad \rho(X) = P^{-1}\begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix}P,$$

et on reconnaît la relation de l'énoncé.

III.2.c. Pour tout $X \in M_n(\mathbb{C})$,

$$\begin{pmatrix} A & B \\ C & D \end{pmatrix} \begin{pmatrix} X & d(X) \\ 0 & X \end{pmatrix} = \begin{pmatrix} X & 0 \\ 0 & X \end{pmatrix} \begin{pmatrix} A & B \\ C & D \end{pmatrix}$$

donc

$$\begin{cases} AX = XA \\ Ad(X) + BX = XB \\ CX = XC \\ Cd(X) + DX = XD. \end{cases}$$

Les seules matrices A qui commutent avec toutes les matrices X de $M_n(\mathbb{C})$ sont des matrices d'homothéties vectorielles, encore appelées matrices scalaires, donc de la forme

$$A = \begin{pmatrix} a & 0 & \cdots & 0 \\ 0 & a & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & & \cdots & a \end{pmatrix} = \operatorname{diag}(a, ..., a)$$

avec $a \in \mathbb{C}$. Il s'agit d'un résultat classique du cours (à savoir : le centre de $\mathrm{GL}(\mathbb{C}^n)$ est formé des homothéties de rapports non nuls, voir [15], Th. 33) que l'on retrouve en appliquant la question II.2 avec $\mathcal{A} = M_n(\mathbb{C}) \simeq \operatorname{End}(\mathbb{C}^n)$.
De même $C = \operatorname{diag}(c, ..., c)$. On ne peut pas avoir $A = C = 0$ car P est bijective, donc $A \neq 0$ ou $B \neq 0$. Si par exemple $A \neq 0$ (l'autre cas se traiterait de la même façon), alors A est une homothétie de rapport non nul, donc inversible, et puisqu'elle commute avec tout le monde :

$$d(X) = A^{-1}(XB - BX) = XA^{-1}B - A^{-1}BX = HX - XH$$

en posant $H = -A^{-1}B$. On obtient bien $d(X) = d_H(X)$ pour tout X, c'est-à-dire $d = d_H$.

Partie IV

IV.1.a. L'application

$$\begin{array}{rccc} \mathrm{Tr}: & M_n(\mathbb{C}) & \to & \mathbb{C} \\ & X = (x_{ij}) & \mapsto & \sum_{i=1}^{n} x_{ii} \end{array}$$

est linéaire, donc pour tous $X = (x_{ij})$, $X' = (x'_{ij})$ et $\lambda \in \mathbb{C}$,

$$\mathrm{Tr}\left((X + \lambda X')Y\right) = \mathrm{Tr}\left(XY + \lambda X'Y\right) = \mathrm{Tr}(XY) + \lambda \, \mathrm{Tr}\left(X'Y\right)$$

c'est-à-dire $\psi(X+\lambda X', Y) = \psi(X,Y) + \lambda\psi(X',Y)$. Cela montre que ψ est linéaire par rapport à la première variable. L'application ψ est symétrique, car si $X = (x_{ij})$ et $Y = (y_{ij})$,

$$\operatorname{Tr}(XY) = \sum_i \sum_k x_{ik}y_{ki} = \sum_k \sum_i y_{ki}x_{ik} = \operatorname{Tr}(YX).$$

Par conséquent, ψ est aussi linéaire par rapport à la seconde variable, donc bilinéaire. Pour terminer, montrer que ψ est non dégénérée revient à montrer que, pour X fixé, l'application linéaire

$$\begin{array}{rccc} \widetilde{\psi}: & M_n(\mathbb{C}) & \to & M_n(\mathbb{C})^* \\ & X & \mapsto & \psi(X,.) \end{array}$$

est injective[3]. Si $X \in \operatorname{Ker}\widetilde{\psi}$,

$$\forall Y \in M_n(\mathbb{C}) \quad \psi(X,Y) = \operatorname{Tr}(XY) = \sum_i \sum_k x_{ik}y_{ki} = 0.$$

Pour tout $(l,c) \in \{1,...,n\}^2$, il suffit de choisir $Y = E_{l,c}$ pour obtenir $x_{cl} = 0$. Ainsi $X = 0$ et $\widetilde{\psi}$ est injective.

Remarque : On peut montrer la non dégénérescence de ψ en considérant $X \in \operatorname{Ker}\widetilde{\psi}$, et en utilisant l'adjointe $X^* = {}^t\overline{X}$ de X, pour calculer

$$\operatorname{Tr}(XX^*) = \sum_{i,k} x_{ik}\overline{x}_{ik} = \sum_{i,k} |x_{ik}|^2.$$

Clairement, $\operatorname{Tr}(XX^*) = 0$ entraîne $X = (x_{ij}) = 0$.

IV.1.b. Soit $(X_1^*, ..., X_{n^2}^*)$ la base duale de $(X_1, ..., X_{n^2})$. Par définition

$$\forall i,j \quad X_j^*(X_i) = \delta_{i,j}.$$

Comme $\widetilde{\psi}$ est un isomorphisme de $M_n(\mathbb{C})$ sur $M_n(\mathbb{C})^*$, toute forme linéaire X_j^* possède un et un seul antécédent par $\widetilde{\psi}$, disons X_j'. Alors $X_j^* = \psi(X_j', .)$ et

$$\forall i,j \quad \psi(X_i, X_j') = \delta_{i,j}.$$

$(X_1', ..., X_{n^2}')$ est une base de $M_n(\mathbb{C})$ comme l'image de la base $(X_1^*, ..., X_{n^2}^*)$ de $M_n(\mathbb{C})^*$ par l'isomorphisme $\widetilde{\psi}^{-1}$.

IV.2. • On a besoin du Lemme suivant :

[3] Ici, on peut aussi dire "bijective" car on est en dimension finie et on sait que $\dim M_n(\mathbb{C}) = \dim M_n(\mathbb{C})^*$. Montrer l'injectivité de $\widetilde{\psi}$ revient à montrer que le seul vecteur de $M_n(\mathbb{C})$ orthogonal à tous les vecteurs de $M_n(\mathbb{C})$ est le vecteur nul, autrement dit que $(M_n(\mathbb{C}))^\perp = \{0\}$. On reconnaît là une autre définition de la non dégénérescence de ψ. Le lecteur pourra retrouver tout ce qu'il faut savoir sur les formes bilinéaires au Chapitre 5 de [15], et particulièrement à la Section 5.1.5 sur la non dégénérescence.

Lemme $\mathbf{\Sigma}$: Pour tout $Y \in M_n(\mathbb{C})$,

$$\begin{cases} Y = \sum_{i=1}^{n^2} \operatorname{Tr}(X_i'Y)\, X_i = \sum_{i=1}^{n^2} \operatorname{Tr}(YX_i')\, X_i \\ Y = \sum_{i=1}^{n^2} \operatorname{Tr}(X_iY)\, X_i' = \sum_{i=1}^{n^2} \operatorname{Tr}(YX_i)\, X_i'. \end{cases}$$

Preuve : Si $Y = \sum_{i=1}^{n^2} \alpha_i X_i$ et $Y = \sum_{i=1}^{n^2} \alpha_i' X_i'$, alors

$$\psi(Y, X_j') = \sum_{i=1}^{n^2} \alpha_i \psi(X_i, X_j') = \alpha_j \ \Rightarrow\ \alpha_j = \operatorname{Tr}(YX_j')$$

$$\text{et} \quad \psi(X_j, Y) = \sum_{i=1}^{n^2} \alpha_i' \psi(X_j, X_i') = \alpha_j' \ \Rightarrow\ \alpha_j' = \operatorname{Tr}(X_jY)\,. \ \blacksquare$$

• Posons $S(A) = \sum_{i=1}^{n^2} X_i A X_i'$, et montrons que $S(A)$ commute avec n'importe quelle matrice Y de $M_n(\mathbb{C})$. Comme seules les homothéties commutent avec tous les endomorphismes de $\mathbb{C}^n$, on pourra affirmer que $S(A)$ est la matrice d'une homothétie, et qu'elle est donc de la forme $S(A) = k_A \mathbf{1}_n$ où $k_A \in \mathbb{C}$.
Le Lemme $\mathbf{\Sigma}$ permet d'écrire :

$$\begin{aligned} S(A)\, Y = \sum_{i=1}^{n^2} X_i A X_i' Y &= \sum_{i=1}^{n^2} X_i A \sum_{j=1}^{n^2} \operatorname{Tr}\left(X_i' Y X_j\right) X_j' \\ &= \sum_{i=1}^{n^2} \sum_{j=1}^{n^2} \operatorname{Tr}\left(X_i' Y X_j\right) X_i A X_j' \\ &= \sum_{j=1}^{n^2} \sum_{i=1}^{n^2} \operatorname{Tr}\left(Y X_j X_i'\right) X_i A X_j' \\ &= \sum_{j=1}^{n^2} Y X_j A X_j' \ = \ Y S(A) \end{aligned}$$

• Pour déterminer k_A, on note que $\operatorname{Tr}(S(A)) = \operatorname{Tr}(k_A \mathbf{1}_n) = n k_A$ et

$$\operatorname{Tr}(S(A)) = \sum_{i=1}^{n^2} \operatorname{Tr}(X_i A X_i') = \sum_{i=1}^{n^2} \operatorname{Tr}(A X_i' X_i) = \operatorname{Tr}\left(\sum_{i=1}^{n^2} A X_i' X_i\right),$$

de sorte que

$$n k_A = \operatorname{Tr}\left(A \sum_{i=1}^{n^2} X_i' X_i\right). \quad (*)$$

En relisant le second point avec $T(A)=\sum_{i=1}^{n^2}X_i'AX_i$ à la place de $S(A)$ (il suffit d'échanger les matrices X_i primées et non primées), on constate qu'il existe toujours un réel k_A' tel que $T(A)=k_A'\mathbf{1}_n$. En particulier

$$T(\mathbf{1}_n)=\sum_{i=1}^{n^2}X_i'X_i=k_{\mathbf{1}_n}'\mathbf{1}_n$$

donc

$$nk_{\mathbf{1}_n}'=\mathrm{Tr}\left(\sum_{i=1}^{n^2}X_i'X_i\right)=\sum_{i=1}^{n^2}\mathrm{Tr}(X_i'X_i)=n^2$$

puisque $\psi(X_i,X_j')=\delta_{i,j}$. On obtient donc $k_{\mathbf{1}_n}'=n$ et

$$\sum_{i=1}^{n^2}X_i'X_i=n\mathbf{1}_n.$$

En remplaçant dans $(*)$, on obtient finalement $nk_A=\mathrm{Tr}(A\times n\mathbf{1}_n)=n\,\mathrm{Tr}(A)$, d'où $k_A=\mathrm{Tr}(A)$ et la formule $S(A)=\sum_{i=1}^{n^2}X_iAX_i'=\mathrm{Tr}(A)\,\mathbf{1}_n$.

Partie V

V.1. g est diagonalisable car annule le polynôme X^m-1 scindé dans $\mathbb{C}$ et n'ayant que des racines simples. Toutes les valeurs propres de g seront des racines m-èmes de l'unité. En effet, si λ est une telle valeur propre et si x désigne un vecteur propre (non nul) associé,

$$g(x)=\lambda x\quad\Rightarrow\quad x=\mathbf{1}_n(x)=g^m(x)=\lambda^m x\quad\Rightarrow\quad\lambda^m=1.$$

Remarques : α) Posons $\omega_k=e^{ik\frac{2\pi}{m}}$. Le Théorème des noyaux appliqué à la décomposition en produit de facteurs irréductibles $X^m-1=\prod_{k=0}^{m-1}(X-\omega_k)$ donne

$$\mathbb{C}^n=\mathrm{Ker}(g^m-\mathbf{1}_n)=\bigoplus_{k=0}^{m-1}\mathrm{Ker}(g-\omega_k\mathbf{1}_n).$$

Cette décomposition montre que g est diagonalisable et exhibe les sous-espaces propres probables. Je dis probables, car il n'y a bien sûr aucune raison pour qu'un noyau donné $\mathrm{Ker}(g-\omega_k\mathbf{1}_n)$ soit distinct de $\{0\}$, et que c'est à cette seule condition qu'on pourra dire qu'il s'agit d'un sous-espace propre de g. On pourra penser à l'homothétie vectorielle h de rapport ω_1 qui vérifie sans doute $h^m=\mathbf{1}_n$ tout en n'admettant qu'un seul sous-espace propre !

β) J'ai identifié $M_n(\mathbb{C})$ et $\mathrm{End}(\mathbb{C}^n)$ comme le propose plus loin l'énoncé. On aurait d'ailleurs déjà dû écrire $g^m = \mathbf{1}_{\mathbb{C}^n}$ au lieu de $g^m = \mathbf{1}_n$ dans le libellé de la propriété (P). Mais cela n'est pas bien grave après l'identification.

V.2. D'après la question précédente, les complexes $\mathrm{Tr}(g)$ seront des sommes de n racines m-èmes de l'unité, qui sont en nombre fini, donc ne prendront qu'un nombre fini de valeurs. L'ensemble $\{\mathrm{Tr}(g),\ g \in G\}$ est donc fini.

V.3.a. Soit V le sous-espace vectoriel engendré par G.

▶ *V est une sous-algèbre unitaire de $M_n(\mathbb{C})$*. En effet, c'est un sous-espace vectoriel de $M_n(\mathbb{C})$, qui contient $\mathbf{1}_n$ (l'élément neutre du groupe G), et on vérifie sans peine que le produit de deux combinaisons linéaires finies d'éléments de G est encore une combinaison linéaire finie d'élément de G.
Vraiment, si les α_i et les β_i sont des complexes, et si les g_i et les h_i appartiennent à G,

$$(\alpha_1 g_1 + ... + \alpha_k g_k)(\beta_1 h_1 + ... + \beta_s h_s) = \sum_{i,j} \alpha_i \beta_j \, g_i h_j$$

avec $g_i h_j \in G$ puisque G est un groupe. Donc cette dernière somme appartient à V.

▶ *V est irréductible* : Un sous-espace F stable par V sera a fortiori stable par G. Comme G est irréductible, F sera égal soit à $\{0\}$, soit à $\mathbb{C}^n$.

▶ Finalement, V est une sous-algèbre unitaire irréductible de $\mathrm{End}(\mathbb{C}^n)$, et la partie II montre que $V = \mathrm{Vect}\{g \,/\, g \in G\} = \mathrm{End}(\mathbb{C}^n)$. On pourra donc toujours trouver une base de $\mathrm{End}(\mathbb{C}^n)$ formée de vecteurs de G (en utilisant le Théorème de la base incomplète).

V.3.b. Soit $(X_1, ..., X_{n^2})$ une base de $M_n(\mathbb{C})$ formée de vecteurs de G. Soit $(X'_1, ..., X'_{n^2})$ la base de $M_n(\mathbb{C})$ construite comme dans la question IV.1. Le Lemme Σ permet d'écrire

$$g = \sum_{i=1}^{n^2} \mathrm{Tr}\left(X'_i g\right) X_i$$

pour tout $g \in G$, de sorte qu'on puisse définir une application injective

$$\begin{array}{rccc} \xi : & G & \to & \Lambda^{n^2} = \Lambda \times ... \times \Lambda \\ & g & \mapsto & (\mathrm{Tr}(X'_1 g), ..., \mathrm{Tr}(X'_{n^2} g)) \end{array}$$

de G dans Λ^{n^2}, où l'on pose $\Lambda = \{\mathrm{Tr}(g),\ g \in G\}$. L'ensemble Λ est fini d'après la question V.2, et ξ est une injection de G dans un ensemble fini. Donc G est fini.

V.4.a. L'énoncé oublie de préciser que p et q ne doivent pas être nuls (sinon la décomposition est triviale conviendrait toujours) et sous-entend que, dans toute cette question, on suppose que G n'est pas irréductible.
Si G n'est pas irréductible, il existe un sous-espace F stable par toutes les applications g de G et de dimension p telle que $1 \leq p \leq n-1$. On choisit un supplémentaire F' de F dans $\mathrm{End}(\mathbb{C}^n)$, une base $(\nu_1 ..., \nu_p)$ de F et une base $(\nu_{p+1} ..., \nu_n)$ de F', et on pose $q = n - p$.
L'inclusion $g(F) \subset F$ vérifiée par *tous* les endomorphismes g de G se traduit, matriciellement, par des 0 dans la matrice de g dans la base $\mathcal{B} = (\nu_1 ..., \nu_n)$ aux i-èmes places et j-èmes colonnes quand $p < i \leq n$ et $j \leq p$. Bref, la matrice de $g \in G$ dans $\mathcal{B}$ est de la forme demandée :

$$\begin{pmatrix} T(g) & U(g) \\ 0 & V(g) \end{pmatrix}.$$

V.4.b. Comme g est inversible, $\det(T(g)) \times \det(V(g)) = \det(g)$ n'est pas nul et les endomorphismes $T(g)$ et $V(g)$ sont inversibles. Le produit

$$g_1 g_2 = \begin{pmatrix} T(g_1) & U(g_1) \\ 0 & V(g_1) \end{pmatrix} \begin{pmatrix} T(g_2) & U(g_2) \\ 0 & V(g_2) \end{pmatrix}$$

de deux éléments de G est égal à

$$\begin{pmatrix} T(g_1)T(g_2) & T(g_1)U(g_2) + U(g_1)V(g_2) \\ 0 & V(g_1)V(g_2) \end{pmatrix},$$

de sorte que

$$\forall g_1, g_2 \in G \quad T(g_1)T(g_2) = T(g_1 g_2) \text{ et } V(g_1)V(g_2) = V(g_1 g_2).$$

Ainsi, les applications $T : G \to \mathrm{GL}(p, \mathbb{C})$ et $V : G \to \mathrm{GL}(q, \mathbb{C})$ sont des homomorphismes de groupes. Comme G_1 et G_2 sont les noyaux de ces morphismes, ce seront des sous-groupes distingués de G.
Si $g \in G_1 \cap G_2$, alors $T(g) = \mathbf{1}_p$, $V(g) = \mathbf{1}_q$ et

$$g^m = \begin{pmatrix} \mathbf{1}_p & mU(g) \\ 0 & \mathbf{1}_q \end{pmatrix} = \mathbf{1}_n,$$

donc $mU(g) = 0$. Par suite $U(g) = 0$, $g = \mathbf{1}_n$ et $G_1 \cap G_2 = \{\mathbf{1}_n\}$.

Remarque : La réponse donnée ci-dessus est rapide. On peut néanmoins se débrouiller sans faire intervenir de noyaux de morphismes de groupes, mais en retournant à la définition d'un sous-groupe distingué. Il s'agit alors de montrer

que pour tout $h \in G_1$ et tout $g \in G$, le produit ghg^{-1} appartient à G_1. On écrit

$$h = \begin{pmatrix} \mathbf{1}_p & A \\ 0 & B \end{pmatrix} \quad \text{et} \quad g = \begin{pmatrix} T & U \\ 0 & V \end{pmatrix}$$

où T et V sont inversibles. On vérifie que

$$g^{-1} = \begin{pmatrix} T^{-1} & -T^{-1}UV^{-1} \\ 0 & V^{-1} \end{pmatrix}$$

(en rafistolant un peu), puis on calcule :

$$gh = \begin{pmatrix} T & U \\ 0 & V \end{pmatrix} \begin{pmatrix} \mathbf{1}_p & A \\ 0 & B \end{pmatrix} = \begin{pmatrix} T & TA+UB \\ 0 & VB \end{pmatrix}$$

$$\begin{aligned} ghg^{-1} &= \begin{pmatrix} T & TA+UB \\ 0 & VB \end{pmatrix} \begin{pmatrix} T^{-1} & -T^{-1}UV^{-1} \\ 0 & V^{-1} \end{pmatrix} \\ &= \begin{pmatrix} \mathbf{1}_p & -UV^{-1}+TAV^{-1}+UBV^{-1} \\ 0 & VBV^{-1} \end{pmatrix}. \end{aligned}$$

Comme ghg^{-1} appartient à G (comme composée d'éléments du groupe G) et $T\left(ghg^{-1}\right) = \mathbf{1}_p$, on a évidemment $ghg^{-1} \in G_1$ et l'affaire est réglée !

V.4.c. L'application

$$\begin{array}{cccc} \Phi : & K & \to & K/K_1 \times K/K_2 \\ & x & \mapsto & (\dot{x}, \overline{x}) \end{array}$$

est un morphisme de groupes de noyau $\operatorname{Ker}\Phi = K_1 \cap K_2$. Par décomposition canonique de Φ, on obtient un morphisme injectif de groupes

$$\widetilde{\Phi} : K/K_1 \cap K_2 \to K/K_1 \times K/K_2.$$

Comme, par hypothèse, K/K_1 et K/K_2 sont finis, $K/(K_1 \cap K_2)$ sera un groupe fini (isomorphe à un sous-groupe de $K/K_1 \times K/K_2$), et $K_1 \cap K_2$ sera bien d'indice fini dans K.

V.4.d. Montrons que G est fini en raisonnant par récurrence sur n.

- Si $n = 1$, le résultat est trivial puisqu'une application g de G est alors dans $\mathrm{GL}(1, \mathbb{C})$, donc est déterminée par l'image d'un vecteur non nul $\overrightarrow{i}$ de $\mathbb{C}$ (qui forme une base de $\mathbb{C}$). Nécessairement $g(\overrightarrow{i}) = \lambda \overrightarrow{i}$ et l'hypothèse $g^m = \mathbf{1}_1$ impose à λ d'être une racine m-ème de l'unité, donc d'appartenir à un ensemble de cardinal m. Dans ce cas le cardinal $|G|$ de G est inférieur ou égal à m.

- Supposons que la propriété soit démontrée jusqu'au rang $n-1$, et considérons un sous-groupe G de $\mathrm{GL}(n,\mathbb{C})$ vérifiant la propriété (P).
De deux choses l'une :

- Si G est irréductible, la question V.3 montre que G est fini.
- Sinon on construit des sous-groupes G_1 et G_2 comme en V.4.b. La décomposition canonique de $T : G \to \mathrm{GL}(p,\mathbb{C})$ montre que G/G_1 est isomorphe à un sous-groupe de $\mathrm{GL}(p,\mathbb{C})$ qui vérifie la condition (P). Comme $p < n$, l'hypothèse récurrente s'applique, et G/G_1 sera un groupe fini. Ainsi G_1 est d'indice fini dans G.

De même G_2 est d'indice fini dans G, et la propriété démontrée en V.4.c montre que $G/(G_1 \cap G_2)$ est fini. Comme $G_1 \cap G_2 = \{0\}$ (d'après V.4.b), on peut affirmer que G est fini.

On vient de démontrer la propriété au rang n.

Partie VI

VI.1. Notons $A * B = (a_{ij}B)_{i,j}$ ou simplement $A * B = (a_{ij}B)$ la matrice $A * B$. C'est une matrice formée de blocs carrés de taille m, et il suffit de faire des produits par blocs pour obtenir (avec des notations évidentes) :

$$\begin{aligned}(A * B)\left(A' * B'\right) &= (a_{ij}B)\,(a'_{ij}B') \\ &= \left(\sum_k a_{ik}B \times a'_{kj}B'\right)_{i,j} \\ &= \left(\left(\sum_k a_{ik}a'_{kj}\right)BB'\right)_{i,j} = AA' * BB'\end{aligned}$$

comme demandé.
Pour tous i, j, l'application

$$\begin{array}{rccc}\varphi_{ij}: & M_n(\mathbb{C}) \times M_m(\mathbb{C}) & \to & M_m(\mathbb{C}) \\ & (A,B) & \mapsto & a_{ij}B\end{array}$$

est clairement bilinéaire, ce qui entraîne la bilinéarité de ϕ. En effet, avec des notations évidentes :

$$\begin{aligned}\phi\left(A+\lambda A', B\right) &= \left(\varphi_{ij}\left(A+\lambda A', B\right)\right)_{i,j} \\ &= \left(\varphi_{ij}(A,B)\right)_{i,j} + \lambda\left(\varphi_{ij}\left(A',B\right)\right)_{i,j} \\ &= \phi(A,B) + \lambda\phi\left(A',B\right),\end{aligned}$$

donc ϕ est linéaire à gauche, et la linéarité à droite se montre de la même façon.

VI.2. Notons $(E_{i,j})$, $(E'_{i,j})$ et $(E''_{i,j})$ les bases canoniques respectives de $M_n(\mathbb{C})$, $M_m(\mathbb{C})$ et $M_{nm}(\mathbb{C})$.

$$\phi(E_{i,j}, E'_{l,c}) = (\delta_{i,j} E'_{l,c})_{i,j}$$

est une matrice dont tous les coefficients sont nuls, excepté un, qui vaut 1, et qui est placé à la $(m\,(i-1)+l)$-ème ligne et $(m\,(j-1)+c)$-ème colonne. Donc

$$\phi(E_{i,j}, E'_{l,c}) = E''_{m(i-1)+l,m(j-1)+c}$$

et toutes les matrices $E''_{i,j}$ de la base canonique de $M_{nm}(\mathbb{C})$ appartiennent à l'image de ϕ. En conclusion $\operatorname{Im}\phi = M_{nm}(\mathbb{C})$.

VI.3.a. On a

$$\begin{aligned} P^2 &= \left(\sum_{1\leq i,j\leq n} E_{i,j} * E_{j,i}\right)\left(\sum_{1\leq l,c\leq n} E_{l,c} * E_{c,l}\right) \\ &= \sum_{i,j,l,c} (E_{i,j} * E_{j,i})\,(E_{l,c} * E_{c,l}) \\ &= \sum_{i,j,l,c} E_{i,j}E_{l,c} * E_{j,i}E_{c,l}. \end{aligned}$$

En utilisant le Lemme E, on obtient

$$\begin{aligned} P^2 &= \sum_{i,j,l,c} \delta_{j,l}\delta_{i,c} E_{i,c} * E_{j,l} \\ &= \sum_{i,j} E_{i,i} * E_{j,j} = \left(\sum_i E_{i,i}\right) * \left(\sum_j E_{j,j}\right) = \mathbf{1}_n * \mathbf{1}_n = \mathbf{1}_{n^2}. \end{aligned}$$

Remarque : Une fois arrivé à l'expression $P^2 = \sum_{i,j} E_{i,i} * E_{j,j}$, on peut ne pas penser à utiliser la bilinéarité de ϕ, et utiliser la formule donnant $\phi(E_{i,j}, E'_{l,c})$ obtenue dans la réponse à la question précédente. On écrit alors :

$$P^2 = \sum_{i,j} E''_{m(i-1)+j,m(i-1)+j} = \sum_{u,v} E''_{u,v} = \mathbf{1}_{n^2}.$$

VI.3.b. On a

$$\begin{aligned} P\,(A*B)\,P &= \sum_{i,j,l,c} (E_{i,j} * E_{j,i})\,(A*B)\,(E_{l,c} * E_{c,l}) \\ &= \sum_{i,j,l,c} (E_{i,j}AE_{l,c}) * (E_{j,i}BE_{c,l}). \quad (\maltese) \end{aligned}$$

• **Première solution :** On calcule $E_{i,j}AE_{l,c}$. Pour cela, on pose

$$\begin{array}{ll} A = (a_{uv}) \ ; & E_{l,c} = (e_{uv}) = (\delta_{u,l}\delta_{v,c}) \ ; \\ AE_{l,c} = (b_{uv}) \ ; & E_{i,j} = (e'_{uv}) = (\delta_{u,i}\delta_{v,j}) \ ; \\ E_{i,j}(AE_{l,c}) = (c_{uv}) \, . & \end{array}$$

On obtient

$$b_{uv} = \sum_k a_{uk}e_{kv} = \sum_k a_{uk}\delta_{k,l}\delta_{v,c} = a_{ul}\delta_{v,c},$$

donc

$$c_{uv} = \sum_s e'_{us}b_{sv} = \sum_s \delta_{u,i}\delta_{s,j}a_{sl}\delta_{v,c} = a_{jl}\delta_{u,i}\delta_{v,c}$$

et

$$E_{i,j}AE_{l,c} = a_{jl}E_{i,c}.$$

En reportant dans (✠),

$$\begin{aligned} P\,(A * B)\,P &= \sum_{i,j,l,c} (a_{jl}E_{i,c}) * (b_{ic}E_{j,l}) \\ &= \left(\sum_{i,c} b_{ic}E_{i,c}\right) * \left(\sum_{j,l} a_{jl}E_{j,l}\right) = B * A. \end{aligned}$$

• **Deuxième solution :** Les deux membres de l'égalité $P\,(A * B)\,P = B * A$ à démontrer sont des fonctions bilinéaires de (A, B). Pour conclure, il suffit donc de démontrer que l'égalité est vraie quand $A = E_{\alpha,\beta}$ et $B = E_{\gamma,\delta}$ (avec des indices quelconques). Si $A = E_{\alpha,\beta}$ et $B = E_{\gamma,\delta}$, la formule (✠) donne

$$P\,(A * B)\,P = \sum_{i,j,l,c} (E_{i,j}E_{\alpha,\beta}E_{l,c}) * (E_{j,i}E_{\gamma,\delta}E_{c,l})$$

et il suffit d'appliquer plusieurs fois le Lemme E pour obtenir

$$\begin{aligned} P\,(A * B)\,P &= \sum_{i,j,l,c} (\delta_{j,\alpha}E_{i,\beta}E_{l,c}) * (\delta_{i,\gamma}E_{j,\delta}E_{c,l}) \\ &= \sum_{i,j,l,c} (\delta_{j,\alpha}\delta_{\beta,l}E_{i,c}) * (\delta_{i,\gamma}\delta_{\delta,c}E_{j,l}) \\ &= E_{\gamma,\delta} * E_{\alpha,\beta} = B * A. \end{aligned}$$

VI.4.a. On a

$$\operatorname{Tr}(A * B) = \sum_{i=1}^{n} \operatorname{Tr}(a_{ii}B) = \left(\sum_{i=1}^{n} a_{ii}\right) \operatorname{Tr}(B) = \operatorname{Tr}(A)\operatorname{Tr}(B)$$

et

$$\det(A * B) = \det(A * \mathbf{1}_n)(\mathbf{1}_n * B) = \det(A * \mathbf{1}_n) \times \det(\mathbf{1}_n * B).$$

La matrice $\mathbf{1}_n * B$ est carrée d'ordre n^2, et diagonale par blocs, avec n blocs égaux à B situés sur la diagonale principale :

$$\mathbf{1}_n * B = \begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & B & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & B \end{pmatrix}.$$

Ainsi $\det(\mathbf{1}_n * B) = (\det B)^n$. Par ailleurs, la question VI.3 montre qu'il existe une matrice involutive P telle que $P(A * B)P = B * A$. Les matrices $A * B$ et $B * A$ sont donc toujours équivalentes. On en déduit

$$\det(A * \mathbf{1}_n) = \det P \times \det(\mathbf{1}_n * A) \times \det P = (\det A)^n$$

et $\det(A * B) = (\det A)^n (\det B)^n$.

VI.4.b. Toute matrice carrée à coefficient dans $\mathbb{C}$ est trigonalisable. Il existe donc des matrices triangulaires supérieures T et S semblables à A et B. Elles s'écrivent

$$T = \begin{pmatrix} \lambda_1 & \# & \cdots & \# \\ 0 & \lambda_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \# \\ 0 & \cdots & 0 & \lambda_n \end{pmatrix} \quad \text{et} \quad S = \begin{pmatrix} \mu_1 & \# & \cdots & \# \\ 0 & \mu_2 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \# \\ 0 & \cdots & 0 & \mu_n \end{pmatrix}$$

où λ_1, ..., λ_n sont les valeurs propres de A, et μ_1, ..., μ_n celles de B (comptées avec leurs ordres de multiplicité dans les polynômes caractéristiques).
Il existe deux matrices inversibles Q et L de $M_n(\mathbb{C})$ telles que $A = Q^{-1}TQ$ et $B = L^{-1}SL$. Alors

$$A * B = \left(Q^{-1}TQ\right) * \left(L^{-1}SL\right) = \left(Q^{-1} * L^{-1}\right)(T * S)(Q * L).$$

Comme

$$\begin{cases} \left(Q^{-1} * L^{-1}\right)(Q * L) = \left(Q^{-1}Q\right) * \left(L^{-1}L\right) = \mathbf{1}_n * \mathbf{1}_n = \mathbf{1}_{n^2} \\ (Q * L)\left(Q^{-1} * L^{-1}\right) = \left(QQ^{-1}\right) * \left(LL^{-1}\right) = \mathbf{1}_n * \mathbf{1}_n = \mathbf{1}_{n^2}, \end{cases}$$

on constate que $Q^{-1} * L^{-1} = (Q * L)^{-1}$, et que

$$A * B = (Q * L)^{-1}(T * S)(Q * L).$$

Ainsi $A*B$, semblable à $T*S$, possédera les mêmes valeurs propres que $T*S$. Mais $T*S$ est une matrice diagonale supérieure dont les coefficients situés sur la diagonale principale sont les $\lambda_i\mu_j$ $(1 \leq i \leq n,\ 1 \leq j \leq n)$. Les valeurs propres de $A*B$ seront donc les produits $\lambda_i\mu_j$ des valeurs propres de A et de B prises deux à deux.

Remarque : On aurait pu utiliser ces matrices triangulaires T et S semblables à A et B pour répondre à la question VI.4.a. En effet, puisque $A*B$ est semblable à $T*S$,

$$\mathrm{Tr}\,(A*B) = \mathrm{Tr}\,(T*S) = \sum_{1\leq i,j\leq n} \lambda_i\mu_j = \left(\sum_{i=1}^{n} \lambda_i\right)\left(\sum_{j=1}^{n} \mu_j\right) = \mathrm{Tr}\,(A)\,\mathrm{Tr}\,(B)$$

et

$$\begin{aligned}
\det\,(A*B) &= \mathrm{Tr}\,(T*S) \\
&= \prod_{1\leq i,j\leq n} \lambda_i\mu_j \\
&= \lambda_1^n...\lambda_n^n\,\mu_1^n...\mu_n^n \\
&= (\lambda_1...\lambda_n)^n\,(\mu_1...\mu_n)^n = \ (\det A)^n\,(\det B)^n\,.
\end{aligned}$$

Bibliographie

[1] G. Auliac, J. Y. Caby. *Analyse pour le Capes et l'Agrégation interne.* Ellipses (2002).

[2] O. Bordelles. *Thèmes d'arithmétique.* Ellipses (2006).

[3] C. Dechamps, A. Warusfel. *Mathématiques tout en un. Série E. Ramis. Volumes 1 et 2.* Dunod. (1999).

[4] J. Dieudonne. *Calcul infinitésimal.* Hermann (1968).

[5] J. Dieudonne. *Eléments d'analyse, tome 1.* Gauthier Villars (1972).

[6] D. Duverney. *Théorie des nombres.* Dunod. (1998).

[7] B. Gostiaux. *Cours de Mathématiques Spéciales. Volumes 1 à 4.* P. U. F. (1995).

[8] X. Gourdon. *Les maths en tête (algèbre).* Ellipses (1994).

[9] X. Gourdon. *Les Maths en tête (analyse).* Ellipses (1994).

[10] G. H. Hardy, E. M. Wright. *An introduction to the theory of numbers.* Oxford (1979).

[11] Y. Hellegouarch. *Invitation aux mathématiques de Fermat-Wiles.* Masson (1997).

[12] S. Lang — *Algèbre.* Dunod (2004).

[13] S. Lang. *Real analysis.* Addison-Wesley (1969).

[14] F. Liret, D. Martinais. *Cours de mathématiques. Analyse 1-ère et 2-ème année.* Dunod (1997).

[15] D.-J. Mercier. *Cours de géométrie, préparation au CAPES et à l'agrégation.* Publibook, 2004.

[16] D.-J. Mercier. *Exercices pour le CAPES mathématiques (externe et interne) & l'agrégation interne, Algèbre, arithmétique et géométrie, Vol. I.* Publibook, 2005.

[17] D.-J. Mercier. *L'épreuve d'exposé au CAPES mathématiques, Leçons rédigées et commentées, Vol. II.* Publibook, 2006.

[18] D.-J. Mercier. *L'épreuve d'exposé au CAPES mathématiques, Leçons rédigées et commentées, Vol. III.* Publibook, 2007.

[19] D.-J. Mercier. *L'épreuve d'exposé au CAPES mathématiques, Leçons rédigées et commentées, Vol. IV.* Publibook, 2008.

[20] D.-J. Mercier. *Exercices pour le CAPES mathématiques (externe et interne) & l'agrégation interne, Algèbre, arithmétique, géométrie et probabilités, Vol. II.* Publibook, 2007.

[21] D. Perrin — *Cours d'Algèbre.* Ellipses (1996).

[22] E. Ramis, C. Deschamps, J. Odoux. *Cours de Mathématiques Spéciales, Volume 1, Algèbre.* Masson, 1989.

[23] E. Ramis, C. Deschamps, J. Odoux. *Cours de Mathématiques Spéciales, Volume 4, Séries et Equations Différentielles.* Masson, 1989.

[24] M. Rogalski. *Carrefours entre analyse algèbre et géométrie.* Ellipses (2001).

[25] J. E. Rombaldi. *Éléments d'analyse réelle.* EDP Sciences (2004).

[26] W. Rudin. *Principes d'analyse mathématique.* Ediscience (1995).